Federal Register

Thursday,
December 28, 2000

Part II

Department of Health and Human Services

Office of the Secretary

45 CFR Parts 160 and 164

Standards for Privacy of Individually Identifiable Health Information; Final Rule

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Parts 160 and 164

Rin: 0991–AB08

Standards for Privacy of Individually Identifiable Health Information

AGENCY: Office of the Assistant Secretary for Planning and Evaluation, DHHS.

ACTION: Final rule.

SUMMARY: This rule includes standards to protect the privacy of individually identifiable health information. The rules below, which apply to health plans, health care clearinghouses, and certain health care providers, present standards with respect to the rights of individuals who are the subjects of this information, procedures for the exercise of those rights, and the authorized and required uses and disclosures of this information.

The use of these standards will improve the efficiency and effectiveness of public and private health programs and health care services by providing enhanced protections for individually identifiable health information. These protections will begin to address growing public concerns that advances in electronic technology and evolution in the health care industry are resulting, or may result, in a substantial erosion of the privacy surrounding individually identifiable health information maintained by health care providers, health plans and their administrative contractors. This rule implements the privacy requirements of the Administrative Simplification subtitle of the Health Insurance Portability and Accountability Act of 1996.

DATES: The final rule is effective on February 26, 2001.

FOR FURTHER INFORMATION CONTACT: Kimberly Coleman, 1–866–OCR–PRIV (1–866–627–7748) or TTY 1–866–788–4989.

SUPPLEMENTARY INFORMATION: Availability of copies, and electronic access.

Copies: To order copies of the **Federal Register** containing this document, send your request to: New Orders, Superintendent of Documents, P.O. Box 371954, Pittsburgh, PA 15250–7954. Specify the date of the issue requested and enclose a check or money order payable to the Superintendent of Documents, or enclose your Visa or Master Card number and expiration date. Credit card orders can also be placed by calling the order desk at (202) 512–1800 or by fax to (202) 512–2250. The cost for each copy is $8.00. As an alternative, you can view and photocopy the **Federal Register** document at most libraries designated as Federal Depository Libraries and at many other public and academic libraries throughout the country that receive the **Federal Register**.

Electronic Access: This document is available electronically at http://aspe.hhs.gov/admnsimp/ as well as at the web site of the Government Printing Office at http://www.access.gpo.gov/su_docs/aces/aces140.html.

I. Background

Table of Contents

Purpose of the Administrative Simplification Regulations

This regulation has three major purposes: (1) To protect and enhance the rights of consumers by providing them access to their health information and controlling the inappropriate use of that information; (2) to improve the quality of health care in the U.S. by restoring trust in the health care system among consumers, health care professionals, and the multitude of organizations and individuals committed to the delivery of care; and (3) to improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection that builds on efforts by states, health systems, and individual organizations and individuals.

This regulation is the second final regulation to be issued in the package of rules mandated under title II subtitle F section 261–264 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104–191, titled ''Administrative Simplification.'' Congress called for steps to improve ''the efficiency and effectiveness of the health care system by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information.'' To achieve that end, Congress required the Department to promulgate a set of interlocking regulations establishing standards and protections for health information systems. The first regulation in this set, Standards for Electronic Transactions 65 FR 50312, was published on August 17, 2000 (the ''Transactions Rule''). This regulation establishing Standards for Privacy of Individually Identifiable Health Information is the second final rule in the package. A rule establishing a unique identifier for employers to use in electronic health care transactions, a rule establishing a unique identifier for providers for such transactions, and a rule establishing standards for the security of electronic information systems have been proposed. See 63 FR 25272 and 25320 (May 7, 1998); 63 FR 32784 (June 16, 1998); 63 FR 43242 (August 12, 1998). Still to be proposed are rules establishing a unique identifier for health plans for electronic transactions, standards for claims attachments, and standards for transferring among health plans appropriate standard data elements needed for coordination of benefits. (See section C, below, for a more detailed explanation of the statutory mandate for these regulations.)

In enacting HIPAA, Congress recognized the fact that administrative simplification cannot succeed if we do not also protect the privacy and confidentiality of personal health information. The provision of high-quality health care requires the exchange of personal, often-sensitive information between an individual and a skilled practitioner. Vital to that interaction is the patient's ability to trust that the information shared will be protected and kept confidential. Yet many patients are concerned that their information is not protected. Among the factors adding to this concern are the growth of the number of organizations involved in the provision of care and the processing of claims, the growing use of electronic information technology, increased efforts to market health care and other products to consumers, and the increasing ability to collect highly sensitive information about a person's current and future health status as a result of advances in scientific research.

Rules requiring the protection of health privacy in the United States have been enacted primarily by the states. While virtually every state has enacted one or more laws to safeguard privacy, these laws vary significantly from state to state and typically apply to only part of the health care system. Many states have adopted laws that protect the health information relating to certain health conditions such as mental illness, communicable diseases, cancer, HIV/AIDS, and other stigmatized conditions. An examination of state health privacy laws and regulations,

however, found that ''state laws, with a few notable exceptions, do not extend comprehensive protections to people's medical records.'' Many state rules fail to provide such basic protections as ensuring a patient's legal right to see a copy of his or her medical record. See Health Privacy Project, ''The State of Health Privacy: An Uneven Terrain,'' Institute for Health Care Research and Policy, Georgetown University (July 1999) (http://www.healthprivacy.org) (the ''Georgetown Study'').

Until now, virtually no federal rules existed to protect the privacy of health information and guarantee patient access to such information. This final rule establishes, for the first time, a set of basic national privacy standards and fair information practices that provides all Americans with a basic level of protection and peace of mind that is essential to their full participation in their care. The rule sets a floor of ground rules for health care providers, health plans, and health care clearinghouses to follow, in order to protect patients and encourage them to seek needed care. The rule seeks to balance the needs of the individual with the needs of the society. It creates a framework of protection that can be strengthened by both the federal government and by states as health information systems continue to evolve.

Need for a National Health Privacy Framework

The Importance of Privacy

Privacy is a fundamental right. As such, it must be viewed differently than any ordinary economic good. The costs and benefits of a regulation must, of course, be considered as a means of identifying and weighing options. At the same time, it is important not to lose sight of the inherent meaning of privacy: it speaks to our individual and collective freedom.

A right to privacy in personal information has historically found expression in American law. All fifty states today recognize in tort law a common law or statutory right to privacy. Many states specifically provide a remedy for public revelation of private facts. Some states, such as California and Tennessee, have a right to privacy as a matter of state constitutional law. The multiple historical sources for legal rights to privacy are traced in many places, including Chapter 13 of Alan Westin's Privacy and Freedom and in Ellen Alderman & Caroline Kennedy, The Right to Privacy (1995).

Throughout our nation's history, we have placed the rights of the individual at the forefront of our democracy. In the Declaration of Independence, we asserted the ''unalienable right'' to ''life, liberty and the pursuit of happiness.'' Many of the most basic protections in the Constitution of the United States are imbued with an attempt to protect individual privacy while balancing it against the larger social purposes of the nation.

To take but one example, the Fourth Amendment to the United States Constitution guarantees that ''the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated.'' By referring to the need for security of ''persons'' as well as ''papers and effects'' the Fourth Amendment suggests enduring values in American law that relate to privacy. The need for security of ''persons'' is consistent with obtaining patient consent before performing invasive medical procedures. The need for security in ''papers and effects'' underscores the importance of protecting information about the person, contained in sources such as personal diaries, medical records, or elsewhere. As is generally true for the right of privacy in information, the right is not absolute. The test instead is what constitutes an ''unreasonable'' search of the papers and effects.

The United States Supreme Court has upheld the constitutional protection of personal health information. In *Whalen* v. *Roe,* 429 U.S. 589 (1977), the Court analyzed a New York statute that created a database of persons who obtained drugs for which there was both a lawful and unlawful market. The Court, in upholding the statute, recognized at least two different kinds of interests within the constitutionally protected ''zone of privacy.'' ''One is the individual interest in avoiding disclosure of personal matters,'' such as this regulation principally addresses. This interest in avoiding disclosure, discussed in Whalen in the context of medical information, was found to be distinct from a different line of cases concerning ''the interest in independence in making certain kinds of important decisions.''

Individuals' right to privacy in information about themselves is not absolute. It does not, for instance, prevent reporting of public health information on communicable diseases or stop law enforcement from getting information when due process has been observed. But many people believe that individuals should have some right to control personal and sensitive information about themselves. Among different sorts of personal information, health information is among the most sensitive. Many people believe that details about their physical self should not generally be put on display for neighbors, employers, and government officials to see. Informed consent laws place limits on the ability of other persons to intrude physically on a person's body. Similar concerns apply to intrusions on information about the person.

Moving beyond these facts of physical treatment, there is also significant intrusion when records reveal details about a person's mental state, such as during treatment for mental health. If, in Justice Brandeis' words, the ''right to be let alone'' means anything, then it likely applies to having outsiders have access to one's intimate thoughts, words, and emotions. In the recent case of *Jaffee* v. *Redmond,* 116 S.Ct. 1923 (1996), the Supreme Court held that statements made to a therapist during a counseling session were protected against civil discovery under the Federal Rules of Evidence. The Court noted that all fifty states have adopted some form of the psychotherapist-patient privilege. In upholding the federal privilege, the Supreme Court stated that it ''serves the public interest by facilitating the appropriate treatment for individuals suffering the effects of a mental or emotional problem. The mental health of our citizenry, no less than its physical health, is a public good of transcendent importance.''

Many writers have urged a philosophical or common-sense right to privacy in one's personal information. Examples include Alan Westin, Privacy and Freedom (1967) and Janna Malamud Smith, Private Matters: In Defense of the Personal Life (1997). These writings emphasize the link between privacy and freedom and privacy and the ''personal life,'' or the ability to develop one's own personality and self-expression. Smith, for instance, states:

> The bottom line is clear. If we continually, gratuitously, reveal other people's privacies, we harm them and ourselves, we undermine the richness of the personal life, and we fuel a social atmosphere of mutual exploitation. Let me put it another way: Little in life is as precious as the freedom to say and do things with people you love that you would not say or do if someone else were present. And few experiences are as fundamental to liberty and autonomy as maintaining control over when, how, to whom, and where you disclose personal material. Id. at 240–241.

In 1890, Louis D. Brandeis and Samuel D. Warren defined the right to privacy as ''the right to be let alone.'' See L. Brandeis, S. Warren, ''The Right

To Privacy,'' 4 Harv.L.Rev. 193. More than a century later, privacy continues to play an important role in Americans' lives. In their book, The Right to Privacy, (Alfred A. Knopf, New York, 1995) Ellen Alderman and Caroline Kennedy describe the importance of privacy in this way:

> Privacy covers many things. It protects the solitude necessary for creative thought. It allows us the independence that is part of raising a family. It protects our right to be secure in our own homes and possessions, assured that the government cannot come barging in. Privacy also encompasses our right to self-determination and to define who we are. Although we live in a world of noisy self-confession, privacy allows us to keep certain facts to ourselves if we so choose. The right to privacy, it seems, is what makes us civilized.

Or, as Cavoukian and Tapscott observed the right of privacy is: ''the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated.'' See A. Cavoukian, D. Tapscott, ''Who Knows: Safeguarding Your Privacy in a Networked World,'' Random House (1995).

Increasing Public Concern About Loss of Privacy

Today, it is virtually impossible for any person to be truly ''let alone.'' The average American is inundated with requests for information from potential employers, retail shops, telephone marketing firms, electronic marketers, banks, insurance companies, hospitals, physicians, health plans, and others. In a 1998 national survey, 88 percent of consumers said they were ''concerned'' by the amount of information being requested, including 55 percent who said they were ''very concerned.'' See Privacy and American Business, 1998 Privacy Concerns & Consumer Choice Survey (http://www.pandab.org). These worries are not just theoretical. Consumers who use the Internet to make purchases or request ''free'' information often are asked for personal and financial information. Companies making such requests routinely promise to protect the confidentiality of that information. Yet several firms have tried to sell this information to other companies even after promising not to do so.

Americans' concern about the privacy of their health information is part of a broader anxiety about their lack of privacy in an array of areas. A series of national public opinion polls conducted by Louis Harris & Associates documents a rising level of public concern about privacy, growing from 64 percent in 1978 to 82 percent in 1995. Over 80 percent of persons surveyed in 1999 agreed with the statement that they had ''lost all control over their personal information.'' See Harris Equifax, Health Information Privacy Study (1993) (http://www.epic.org/privacy/medical/polls.html). A Wall Street Journal/ABC poll on September 16, 1999 asked Americans what concerned them most in the coming century. ''Loss of personal privacy'' was the first or second concern of 29 percent of respondents. All other issues, such a terrorism, world war, and global warming had scores of 23 percent or less.

This growing concern stems from several trends, including the growing use of interconnected electronic media for business and personal activities, our increasing ability to know an individual's genetic make-up, and, in health care, the increasing complexity of the system. Each of these trends brings the potential for tremendous benefits to individuals and society generally. At the same time, each also brings new potential for invasions of our privacy.

Increasing Use of Interconnected Electronic Information Systems

Until recently, health information was recorded and maintained on paper and stored in the offices of community-based physicians, nurses, hospitals, and other health care professionals and institutions. In some ways, this imperfect system of record keeping created a false sense of privacy among patients, providers, and others. Patients' health information has never remained completely confidential. Until recently, however, a breach of confidentiality involved a physical exchange of paper records or a verbal exchange of information. Today, however, more and more health care providers, plans, and others are utilizing electronic means of storing and transmitting health information. In 1996, the health care industry invested an estimated $10 billion to $15 billion on information technology. See National Research Council, Computer Science and Telecommunications Board, ''For the Record: Protecting Electronic Health Information,'' (1997). The electronic information revolution is transforming the recording of health information so that the disclosure of information may require only a push of a button. In a matter of seconds, a person's most profoundly private information can be shared with hundreds, thousands, even millions of individuals and organizations at a time. While the majority of medical records still are in paper form, information from those records is often copied and transmitted through electronic means.

This ease of information collection, organization, retention, and exchange made possible by the advances in computer and other electronic technology affords many benefits to individuals and to the health care industry. Use of electronic information has helped to speed the delivery of effective care and the processing of billions of dollars worth of health care claims. Greater use of electronic data has also increased our ability to identify and treat those who are at risk for disease, conduct vital research, detect fraud and abuse, and measure and improve the quality of care delivered in the U.S. The National Research Council recently reported that ''the Internet has great potential to improve Americans'' health by enhancing communications and improving access to information for care providers, patients, health plan administrators, public health officials, biomedical researchers, and other health professionals.'' See ''Networking Health: Prescriptions for the Internet,'' National Academy of Sciences (2000).

At the same time, these advances have reduced or eliminated many of the financial and logistical obstacles that previously served to protect the confidentiality of health information and the privacy interests of individuals. And they have made our information available to many more people. The shift from paper to electronic records, with the accompanying greater flows of sensitive health information, thus strengthens the arguments for giving legal protection to the right to privacy in health information. In an earlier period where it was far more expensive to access and use medical records, the risk of harm to individuals was relatively low. In the potential near future, when technology makes it almost free to send lifetime medical records over the Internet, the risks may grow rapidly. It may become cost-effective, for instance, for companies to offer services that allow purchasers to obtain details of a person's physical and mental treatments. In addition to legitimate possible uses for such services, malicious or inquisitive persons may download medical records for purposes ranging from identity theft to embarrassment to prurient interest in the life of a celebrity or neighbor. The comments to the proposed privacy rule indicate that many persons believe that they have a right to live in society without having these details of their lives laid open to unknown and possibly hostile eyes. These technological changes, in short, may provide a reason for institutionalizing

privacy protections in situations where the risk of harm did not previously justify writing such protections into law.

The growing level of trepidation about privacy in general, noted above, has tracked the rise in electronic information technology. Americans have embraced the use of the Internet and other forms of electronic information as a way to provide greater access to information, save time, and save money. For example, 60 percent of Americans surveyed in 1999 reported that they have a computer in their home; 82 percent reported that they have used a computer; 64 percent say they have used the Internet; and 58 percent have sent an e-mail. Among those who are under the age of 60, these percentages are even higher. See ''National Survey of Adults on Technology,'' Henry J. Kaiser Family Foundation (February, 2000). But 59 percent of Americans reported that they worry that an unauthorized person will gain access to their information. A recent survey suggests that 75 percent of consumers seeking health information on the Internet are concerned or very concerned about the health sites they visit sharing their personal health information with a third party without their permission. Ethics Survey of Consumer Attitudes about Health Web Sites, California Health Care Foundation, at 3 (January, 2000).

Unless public fears are allayed, we will be unable to obtain the full benefits of electronic technologies. The absence of national standards for the confidentiality of health information has made the health care industry and the population in general uncomfortable about this primarily financially-driven expansion in the use of electronic data. Many plans, providers, and clearinghouses have taken steps to safeguard the privacy of individually identifiable health information. Yet they must currently rely on a patchwork of State laws and regulations that are incomplete and, at times, inconsistent. States have, to varying degrees, attempted to enhance confidentiality by establishing laws governing at least some aspects of medical record privacy. This approach, though a step in the right direction, is inadequate. These laws fail to provide a consistent or comprehensive legal foundation of health information privacy. For example, there is considerable variation among the states in the type of information protected and the scope of the protections provided. See Georgetown Study, at Executive Summary; Lawrence O. Gostin, Zita Lazzarrini, Kathleen M. Flaherty, Legislative Survey of State Confidentiality Laws, with Specific Emphasis on HIV and Immunization, Report to Centers for Disease Control, Council of State and Territorial Epidemiologists, and Task Force for Child Survival and Development, Carter Presidential Center (1996) (Gostin Study).

Moreover, electronic health data is becoming increasingly ''national''; as more information becomes available in electronic form, it can have value far beyond the immediate community where the patient resides. Neither private action nor state laws provide a sufficiently comprehensive and rigorous legal structure to allay public concerns, protect the right to privacy, and correct the market failures caused by the absence of privacy protections (see discussion below of market failure under section V.C). Hence, a national policy with consistent rules is necessary to encourage the increased and proper use of electronic information while also protecting the very real needs of patients to safeguard their privacy.

Advances in Genetic Sciences

Recently, scientists completed nearly a decade of work unlocking the mysteries of the human genome, creating tremendous new opportunities to identify and prevent many of the leading causes of death and disability in this country and around the world. Yet the absence of privacy protections for health information endanger these efforts by creating a barrier of distrust and suspicion among consumers. A 1995 national poll found that more than 85 percent of those surveyed were either ''very concerned'' or ''somewhat concerned'' that insurers and employers might gain access to and use genetic information. See Harris Poll, 1995 #34. Sixty-three percent of the 1,000 participants in a 1997 national survey said they would not take genetic tests if insurers and employers could gain access to the results. See ''Genetic Information and the Workplace,'' Department of Labor, Department of Health and Human Services, Equal Employment Opportunity Commission, January 20, 1998. ''In genetic testing studies at the National Institutes of Health, thirty-two percent of eligible people who were offered a test for breast cancer risk declined to take it, citing concerns about loss of privacy and the potential for discrimination in health insurance.'' Sen. Leahy's comments for March 10, 1999 Introduction of the Medical Information Privacy and Security Act.

The Changing Health Care System

The number of entities who are maintaining and transmitting individually identifiable health information has increased significantly over the last 10 years. In addition, the rapid growth of integrated health care delivery systems requires greater use of integrated health information systems. The health care industry has been transformed from one that relied primarily on one-on-one interactions between patients and clinicians to a system of integrated health care delivery networks and managed care providers. Such a system requires the processing and collection of information about patients and plan enrollees (for example, in claims files or enrollment records), resulting in the creation of databases that can be easily transmitted. This dramatic change in the practice of medicine brings with it important prospects for the improvement of the quality of care and reducing the cost of that care. It also, however, means that increasing numbers of people have access to health information. And, as health plan functions are increasingly outsourced, a growing number of organizations not affiliated with our physicians or health plans also have access to health information.

According to the American Health Information Management Association (AHIMA), an average of 150 people ''from nursing staff to x-ray technicians, to billing clerks'' have access to a patient's medical records during the course of a typical hospitalization. While many of these individuals have a legitimate need to see all or part of a patient's records, no laws govern who those people are, what information they are able to see, and what they are and are not allowed to do with that information once they have access to it. According to the National Research Council, individually identifiable health information frequently is shared with:

- Consulting physicians;
- Managed care organizations;
- Health insurance companies
- Life insurance companies;
- Self-insured employers;
- Pharmacies;
- Pharmacy benefit managers;
- Clinical laboratories;
- Accrediting organizations;
- State and Federal statistical agencies; and
- Medical information bureaus.

Much of this sharing of information is done without the knowledge of the patient involved. While many of these functions are important for smooth functioning of the health care system, there are no rules governing how that

information is used by secondary and tertiary users. For example, a pharmacy benefit manager could receive information to determine whether an insurance plan or HMO should cover a prescription, but then use the information to market other products to the same patient. Similarly, many of us obtain health insurance coverage though our employer and, in some instances, the employer itself acts as the insurer. In these cases, the employer will obtain identifiable health information about its employees as part of the legitimate health insurance functions such as claims processing, quality improvement, and fraud detection activities. At the same time, there is no comprehensive protection prohibiting the employer from using that information to make decisions about promotions or job retention.

Public concerns reflect these developments. A 1993 Lou Harris poll found that 75 percent of those surveyed worry that medical information from a computerized national health information system will be used for many non-health reasons, and 38 percent are very concerned. This poll, taken during the health reform efforts of 1993, showed that 85 percent of respondents believed that protecting the confidentiality of medical records is ''absolutely essential'' or ''very essential'' in health care reform. An ACLU Poll in 1994 also found that 75 percent of those surveyed are concerned a ''great deal'' or a ''fair amount''' about insurance companies putting medical information about them into a computer information bank to which others have access. Harris Equifax, Health Information Privacy Study 2,33 (1993) http://www.epic.org/privacy/medical/poll.html. Another survey found that 35 percent of Fortune 500 companies look at people's medical records before making hiring and promotion decisions. Starr, Paul. ''Health and the Right to Privacy,'' American Journal of Law and Medicine, 1999. Vol 25, pp. 193–201.

Concerns about the lack of attention to information privacy in the health care industry are not merely theoretical. In the absence of a national legal framework of health privacy protections, consumers are increasingly vulnerable to the exposure of their personal health information. Disclosure of individually identifiable information can occur deliberately or accidentally and can occur within an organization or be the result of an external breach of security. Examples of recent privacy breaches include:

- A Michigan-based health system accidentally posted the medical records of thousands of patients on the Internet (The Ann Arbor News, February 10, 1999).
- A Utah-based pharmaceutical benefits management firm used patient data to solicit business for its owner, a drug store (Kiplingers, February 2000).
- An employee of the Tampa, Florida, health department took a computer disk containing the names of 4,000 people who had tested positive for HIV, the virus that causes AIDS (USA Today, October 10, 1996).
- The health insurance claims forms of thousands of patients blew out of a truck on its way to a recycling center in East Hartford, Connecticut (The Hartford Courant, May 14, 1999).
- A patient in a Boston-area hospital discovered that her medical record had been read by more than 200 of the hospital's employees (The Boston Globe, August 1, 2000).
- A Nevada woman who purchased a used computer discovered that the computer still contained the prescription records of the customers of the pharmacy that had previously owned the computer. The pharmacy data base included names, addresses, social security numbers, and a list of all the medicines the customers had purchased. (The New York Times, April 4, 1997 and April 12, 1997).
- A speculator bid $4000 for the patient records of a family practice in South Carolina. Among the businessman's uses of the purchased records was selling them back to the former patients. (New York Times, August 14, 1991).
- In 1993, the Boston Globe reported that Johnson and Johnson marketed a list of 5 million names and addresses of elderly incontinent women. (ACLU Legislative Update, April 1998).
- A few weeks after an Orlando woman had her doctor perform some routine tests, she received a letter from a drug company promoting a treatment for her high cholesterol. (Orlando Sentinel, November 30, 1997).

No matter how or why a disclosure of personal information is made, the harm to the individual is the same. In the face of industry evolution, the potential benefits of our changing health care system, and the real risks and occurrences of harm, protection of privacy must be built into the routine operations of our health care system.

Privacy Is Necessary To Secure Effective, High Quality Health Care

While privacy is one of the key values on which our society is built, it is more than an end in itself. It is also necessary for the effective delivery of health care, both to individuals and to populations. The market failures caused by the lack of effective privacy protections for health information are discussed below (see section V.C below). Here, we discuss how privacy is a necessary foundation for delivery of high quality health care. In short, the entire health care system is built upon the willingness of individuals to share the most intimate details of their lives with their health care providers.

The need for privacy of health information, in particular, has long been recognized as critical to the delivery of needed medical care. More than anything else, the relationship between a patient and a clinician is based on trust. The clinician must trust the patient to give full and truthful information about their health, symptoms, and medical history. The patient must trust the clinician to use that information to improve his or her health and to respect the need to keep such information private. In order to receive accurate and reliable diagnosis and treatment, patients must provide health care professionals with accurate, detailed information about their personal health, behavior, and other aspects of their lives. The provision of health information assists in the diagnosis of an illness or condition, in the development of a treatment plan, and in the evaluation of the effectiveness of that treatment. In the absence of full and accurate information, there is a serious risk that the treatment plan will be inappropriate to the patient's situation.

Patients also benefit from the disclosure of such information to the health plans that pay for and can help them gain access to needed care. Health plans and health care clearinghouses rely on the provision of such information to accurately and promptly process claims for payment and for other administrative functions that directly affect a patient's ability to receive needed care, the quality of that care, and the efficiency with which it is delivered.

Accurate medical records assist communities in identifying troubling public health trends and in evaluating the effectiveness of various public health efforts. Accurate information helps public and private payers make correct payments for care received and lower costs by identifying fraud. Accurate information provides scientists with data they need to conduct research. We cannot improve the quality of health care without information about which treatments work, and which do not.

Individuals cannot be expected to share the most intimate details of their lives unless they have confidence that such information will not be used or

shared inappropriately. Privacy violations reduce consumers' trust in the health care system and institutions that serve them. Such a loss of faith can impede the quality of the health care they receive, and can harm the financial health of health care institutions.

Patients who are worried about the possible misuse of their information often take steps to protect their privacy. Recent studies show that a person who does not believe his privacy will be protected is much less likely to participate fully in the diagnosis and treatment of his medical condition. A national survey conducted in January 1999 found that one in five Americans believe their health information is being used inappropriately. See California HealthCare Foundation, ''National Survey: Confidentiality of Medical Records'' (January, 1999) (http://www.chcf.org). More troubling is the fact that one in six Americans reported that they have taken some sort of evasive action to avoid the inappropriate use of their information by providing inaccurate information to a health care provider, changing physicians, or avoiding care altogether. Similarly, in its comments on our proposed rule, the Association of American Physicians and Surgeons reported 78 percent of its members reported withholding information from a patient's record due to privacy concerns and another 87 percent reported having had a patient request to withhold information from their records. For an example of this phenomenon in a particular demographic group, see Drs. Bearman, Ford, and Moody, ''Foregone Health Care among Adolescents,'' JAMA, vol. 282, no. 23 (999); Cheng, T.L., et al., ''Confidentiality in Health Care: A Survey of Knowledge, Perceptions, and Attitudes among High School Students,'' JAMA, vol. 269, no. 11 (1993), at 1404–1407.

The absence of strong national standards for medical privacy has widespread consequences. Health care professionals who lose the trust of their patients cannot deliver high-quality care. In 1999, a coalition of organizations representing various stakeholders including health plans, physicians, nurses, employers, disability and mental health advocates, accreditation organizations as well as experts in public health, medical ethics, information systems, and health policy adopted a set of ''best principles'' for health care privacy that are consistent with the standards we lay out here. (See the Health Privacy Working Group, ''Best Principles for Health Privacy'' (July, 1999) (Best Principles Study). The Best Principles Study states that—

> To protect their privacy and avoid embarrassment, stigma, and discrimination, some people withhold information from their health care providers, provide inaccurate information, doctor-hop to avoid a consolidated medical record, pay out-of-pocket for care that is covered by insurance, and—in some cases—avoid care altogether.

Best Principles Study, at 9. In their comments on our proposed rule, numerous organizations representing health plans, health providers, employers, and others acknowledged the value of a set of national privacy standards to the efficient operation of their practices and businesses.

Breaches of Health Privacy Harm More Than Our Health Status

A breach of a person's health privacy can have significant implications well beyond the physical health of that person, including the loss of a job, alienation of family and friends, the loss of health insurance, and public humiliation. For example:

- A banker who also sat on a county health board gained access to patients' records and identified several people with cancer and called in their mortgages. See the National Law Journal, May 30, 1994.
- A physician was diagnosed with AIDS at the hospital in which he practiced medicine. His surgical privileges were suspended. See *Estate of Behringer* v. *Medical Center at Princeton,* 249 N.J. Super. 597.
- A candidate for Congress nearly saw her campaign derailed when newspapers published the fact that she had sought psychiatric treatment after a suicide attempt. See New York Times, October 10, 1992, Section 1, page 25.
- A 30-year FBI veteran was put on administrative leave when, without his permission, his pharmacy released information about his treatment for depression. (Los Angeles Times, September 1, 1998) Consumer Reports found that 40 percent of insurers disclose personal health information to lenders, employers, or marketers without customer permission. ''Who's reading your Medical Records,'' Consumer Reports, October 1994, at 628, paraphrasing Sweeny, Latanya, ''Weaving Technology and Policy Together to Maintain Confidentiality,'' The Journal Of Law Medicine and Ethics (Summer & Fall 1997) Vol. 25, Numbers 2,3.

The answer to these concerns is not for consumers to withdraw from society and the health care system, but for society to establish a clear national legal framework for privacy. By spelling out what is and what is not an allowable use of a person's identifiable health information, such standards can help to restore and preserve trust in the health care system and the individuals and institutions that comprise that system. As medical historian Paul Starr wrote: ''Patients have a strong interest in preserving the privacy of their personal health information but they also have an interest in medical research and other efforts by health care organizations to improve the medical care they receive. As members of the wider community, they have an interest in public health measures that require the collection of personal data.'' (P. Starr, ''Health and the Right to Privacy,'' American Journal of Law & Medicine, 25, nos. 2&3 (1999) 193–201). The task of society and its government is to create a balance in which the individual's needs and rights are balanced against the needs and rights of society as a whole.

National standards for medical privacy must recognize the sometimes competing goals of improving individual and public health, advancing scientific knowledge, enforcing the laws of the land, and processing and paying claims for health care services. This need for balance has been recognized by many of the experts in this field. Cavoukian and Tapscott described it this way: ''An individual's right to privacy may conflict with the collective rights of the public * * *. We do not suggest that privacy is an absolute right that reigns supreme over all other rights. It does not. However, the case for privacy will depend on a number of factors that can influence the balance—the level of harm to the individual involved versus the needs of the public.''

The Federal Response

There have been numerous federal initiatives aimed at protecting the privacy of especially sensitive personal information over the past several years—and several decades. While the rules below are likely the largest single federal initiative to protect privacy, they are by no means alone in the field. Rather, the rules arrive in the context of recent legislative activity to grapple with advances in technology, in addition to an already established body of law granting federal protections for personal privacy.

In 1965, the House of Representatives created a Special Subcommittee on Invasion of Privacy. In 1973, this Department's predecessor agency, the Department of Health, Education and Welfare issued The Code of Fair Information Practice Principles establishing an important baseline for

information privacy in the U.S. These principles formed the basis for the federal Privacy Act of 1974, which regulates the government's use of personal information by limiting the disclosure of personally-identifiable information, allows consumers access to information about them, requires federal agencies to specify the purposes for collecting personal information, and provides civil and criminal penalties for misuse of information.

In the last several years, with the rapid expansion in electronic technology—and accompanying concerns about individual privacy—laws, regulations, and legislative proposals have been developed in areas ranging from financial privacy to genetic privacy to the safeguarding of children on-line. For example, the Children's Online Privacy Protection Act was enacted in 1998, providing protection for children when interacting at web-sites. In February, 2000, President Clinton signed Executive Order 13145, banning the use of genetic information in federal hiring and promotion decisions. The landmark financial modernization bill, signed by the President in November, 1999, likewise contained financial privacy protections for consumers. There also has been recent legislative activity on establishing legal safeguards for the privacy of individuals' Social Security numbers, and calls for regulation of on-line privacy in general.

These most recent laws, regulations, and legislative proposals come against the backdrop of decades of privacy-enhancing statutes passed at the federal level to enact safeguards in fields ranging from government data files to video rental records. In the 1970s, individual privacy was paramount in the passage of the Fair Credit Reporting Act (1970), the Privacy Act (1974), the Family Educational Rights and Privacy Act (1974), and the Right to Financial Privacy Act (1978). These key laws were followed in the next decade by another series of statutes, including the Privacy Protection Act (1980), the Electronic Communications Privacy Act (1986), the Video Privacy Protection Act (1988), and the Employee Polygraph Protection Act (1988). In the last ten years, Congress and the President have passed additional legal privacy protection through, among others, the Telephone Consumer Protection Act (1991), the Driver's Privacy Protection Act (1994), the Telecommunications Act (1996), the Children's Online Privacy Protection Act (1998), the Identity Theft and Assumption Deterrence Act (1998), and Title V of the Gramm-Leach-Bliley Act (1999) governing financial privacy.

In 1997, a Presidential advisory commission, the Advisory Commission on Consumer Protection and Quality in the Health Care Industry, recognized the need for patient privacy protection in its recommendations for a Consumer Bill of Rights and Responsibilities (November 1997). In 1997, Congress enacted the Balanced Budget Act (Public Law 105–34), which added language to the Social Security Act (18 U.S.C. 1852) to require Medicare+Choice organizations to establish safeguards for the privacy of individually identifiable patient information. Similarly, the Veterans Benefits section of the U.S. Code provides for confidentiality of medical records in cases involving drug abuse, alcoholism or alcohol abuse, HIV infection, or sickle cell anemia (38 U.S.C. 7332).

As described in more detail in the next section, Congress recognized the importance of protecting the privacy of health information by enacting the Health Insurance Portability and Accountability Act of 1996. The Act called on Congress to enact a medical privacy statute and asked the Secretary of Health and Human Services to provide Congress with recommendations for protecting the confidentiality of health care information. The Congress further recognized the importance of such standards by providing the Secretary with authority to promulgate regulations on health care privacy in the event that lawmakers were unable to act within the allotted three years.

Finally, it also is important for the U.S. to join the rest of the developed world in establishing basic medical privacy protections. In 1995, the European Union (EU) adopted a Data Privacy Directive requiring its 15 member states to adopt consistent privacy laws by October 1998. The EU urged all other nations to do the same or face the potential loss of access to information from EU countries.

Statutory Background

History of the Privacy Component of the Administrative Simplification Provisions

The Congress addressed the opportunities and challenges presented by the rapid evolution of health information systems in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104–191, which was enacted on August 21, 1996. Sections 261 through 264 of HIPAA are known as the Administrative Simplification provisions. The major part of these Administrative Simplification provisions are found at section 262 of HIPAA, which enacted a new part C of title XI of the Social Security Act (hereinafter we refer to the Social Security Act as the ''Act'' and we refer to all other laws cited in this document by their names).

In section 262, Congress primarily sought to facilitate the efficiencies and cost savings for the health care industry that the increasing use of electronic technology affords. Thus, section 262 directs HHS to issue standards to facilitate the electronic exchange of information with respect to financial and administrative transactions carried out by health plans, health care clearinghouses, and health care providers who transmit information electronically in connection with such transactions.

At the same time, Congress recognized the challenges to the confidentiality of health information presented by the increasing complexity of the health care industry, and by advances in health information systems technology and communications. Section 262 thus also directs HHS to develop standards to protect the security, including the confidentiality and integrity, of health information.

Congress has long recognized the need for protection of health information privacy generally, as well as the privacy implications of electronic data interchange and the increased ease of transmitting and sharing individually identifiable health information. Congress has been working on broad health privacy legislation for many years and, as evidenced by the self-imposed three year deadline included in the HIPAA, discussed below, believes it can and should enact such legislation. A significant portion of the first Administrative Simplification section debated on the floor of the Senate in 1994 (as part of the Health Security Act) consisted of privacy provisions. In the version of the HIPAA passed by the House of Representatives in 1996, the requirement for the issuance of privacy standards was located in the same section of the bill (section 1173) as the requirements for issuance of the other HIPAA Administrative Simplification standards. In conference, the requirement for privacy standards was moved to a separate section in the same part of HIPAA, section 264, so that Congress could link the Privacy standards to Congressional action.

Section 264(b) requires the Secretary of HHS to develop and submit to the Congress recommendations for:

- The rights that an individual who is a subject of individually identifiable health information should have.

• The procedures that should be established for the exercise of such rights.

• The uses and disclosures of such information that should be authorized or required.

The Secretary's Recommendations were submitted to the Congress on September 11, 1997. Section 264(c)(1) provides that:

> If legislation governing standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a) of the Social Security Act (as added by section 262) is not enacted by [August 21, 1999], the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than [February 21, 2000]. Such regulations shall address at least the subjects described in subsection (b).

As the Congress did not enact legislation regarding the privacy of individually identifiable health information prior to August 21, 1999, HHS published proposed rules setting forth such standards on November 3, 1999, 64 FR 59918, and is now publishing the mandated final regulation.

These privacy standards have been, and continue to be, an integral part of the suite of Administrative Simplification standards intended to simplify and improve the efficiency of the administration of our health care system.

The Administrative Simplification Provisions, and Regulatory Actions to Date

Part C of title XI consists of sections 1171 through 1179 of the Act. These sections define various terms and impose several requirements on HHS, health plans, health care clearinghouses, and health care providers who conduct the identified transactions electronically.

The first section, section 1171 of the Act, establishes definitions for purposes of part C of title XI for the following terms: code set, health care clearinghouse, health care provider, health information, health plan, individually identifiable health information, standard, and standard setting organization.

Section 1172 of the Act makes the standard adopted under part C applicable to: (1) Health plans, (2) health care clearinghouses, and (3) health care providers who transmit health information in electronic form in connection with transactions referred to in section 1173(a)(1) of the Act (hereinafter referred to as the ''covered entities''). Section 1172 also contains procedural requirements concerning the adoption of standards, including the role of standard setting organizations and required consultations, summarized in subsection F and section VI, below.

Section 1173 of the Act requires the Secretary to adopt standards for transactions, and data elements for such transactions, to enable health information to be exchanged electronically. Section 1173(a)(1) describes the transactions to be promulgated, which include the nine transactions listed in section 1173(a)(2) and other transactions determined appropriate by the Secretary. The remainder of section 1173 sets out requirements for the specific standards the Secretary is to adopt: Unique health identifiers, code sets, security standards, electronic signatures, and transfer of information among health plans. Of particular relevance to this proposed rule is section 1173(d), the security standard provision. The security standard authority applies to both the transmission and the maintenance of health information, and requires the entities described in section 1172(a) to maintain reasonable and appropriate safeguards to ensure the integrity and confidentiality of the information, protect against reasonably anticipated threats or hazards to the security or integrity of the information or unauthorized uses or disclosures of the information, and to ensure compliance with part C by the entity's officers and employees.

In section 1174 of the Act, the Secretary is required to establish standards for all of the above transactions, except claims attachments, by February 21, 1998. The statutory deadline for the claims attachment standard is February 21, 1999.

As noted above, a proposed rule for most of the transactions was published on May 7, 1998, and the final Transactions Rule was promulgated on August 17, 2000. The delay was caused by the deliberate consensus building process, working with industry, and the large number of comments received (about 17,000). In addition, in a series of Notices of Proposed Rulemakings, HHS published other proposed standards, as described above. Each of these steps was taken in concert with the affected professions and industries, to ensure rapid adoption and compliance.

Generally, after a standard is established, it may not be changed during the first year after adoption except for changes that are necessary to permit compliance with the standard. Modifications to any of these standards may be made after the first year, but not more frequently than once every 12 months. The Secretary also must ensure that procedures exist for the routine maintenance, testing, enhancement, and expansion of code sets and that there are crosswalks from prior versions.

Section 1175 of the Act prohibits health plans from refusing to process, or from delaying processing of, a transaction that is presented in standard format. It also establishes a timetable for compliance: each person to whom a standard or implementation specification applies is required to comply with the standard within 24 months (or 36 months for small health plans) of its adoption. A health plan or other entity may, of course, comply voluntarily before the effective date. The section also provides that compliance with modifications to standards or implementation specifications must be accomplished by a date designated by the Secretary, which date may not be earlier than 180 days from the notice of change.

Section 1176 of the Act establishes civil monetary penalties for violation of the provisions in part C of title XI of the Act, subject to several limitations. Penalties may not be more than $100 per person per violation and not more than $25,000 per person for violations of a single standard for a calendar year. The procedural provisions of section 1128A of the Act apply to actions taken to obtain civil monetary penalties under this section.

Section 1177 establishes penalties for any person that knowingly uses a unique health identifier, or obtains or discloses individually identifiable health information in violation of the part. The penalties include: (1) A fine of not more than $50,000 and/or imprisonment of not more than 1 year; (2) if the offense is ''under false pretenses,'' a fine of not more than $100,000 and/or imprisonment of not more than 5 years; and (3) if the offense is with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a fine of not more than $250,000 and/or imprisonment of not more than 10 years.

Under section 1178 of the Act, the requirements of part C, as well as any standards or implementation specifications adopted thereunder, preempt contrary state law. There are three exceptions to this general rule of preemption: State laws that the Secretary determines are necessary for certain purposes set forth in the statute; state laws that the Secretary determines address controlled substances; and state laws relating to the privacy of

individually identifiable health information that are contrary to and more stringent than the federal requirements. There also are certain areas of state law (generally relating to public health and oversight of health plans) that are explicitly carved out of the general rule of preemption and addressed separately.

Section 1179 of the Act makes the above provisions inapplicable to financial institutions (as defined by section 1101 of the Right to Financial Privacy Act of 1978) or anyone acting on behalf of a financial institution when ''authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments for a financial institution.''

Finally, as explained above, section 264 requires the Secretary to issue standards with respect to the privacy of individually identifiable health information. Section 264 also contains a preemption provision that provides that contrary provisions of state laws that are more stringent than the federal standards, requirements, or implementation specifications will not be preempted.

Our Approach to This Regulation

Balance

A number of facts informed our approach to this regulation. Determining the best approach to protecting privacy depends on where we start, both with respect to existing legal expectations and also with respect to the expectations of individuals, health care providers, payers and other stakeholders. From the comments we received on the proposed rule, and from the extensive fact finding in which we engaged, a confused picture developed. We learned that stakeholders in the system have very different ideas about the extent and nature of the privacy protections that exist today, and very different ideas about appropriate uses of health information. This leads us to seek to balance the views of the different stakeholders, weighing the varying interests on each particular issue with a view to creating balance in the regulation as a whole.

For example, we received hundreds of comments explaining the legitimacy of various uses and disclosure of health information. We agree that many uses and disclosures of health information are ''legitimate,'' but that is not the end of the inquiry. Neither privacy, nor the important social goals described by the commenters, are absolutes. In this regulation, we are asking health providers and institutions to add privacy into the balance, and we are asking individuals to add social goals into the balance.

The vast difference among regulated entities also informed our approach in significant ways. This regulation applies to solo practitioners, and multi-national health plans. It applies to pharmacies and information clearinghouses. These entities differ not only in the nature and scope of their businesses, but also in the degree of sophistication of their information systems and information needs. We therefore designed the core requirements of this regulation to be flexible and ''scalable.'' This is reflected throughout the rule, particularly in the implementation specifications for making the minimum necessary uses and disclosures, and in the administrative policies and procedures requirements.

We also are informed by the rapid evolution in industry organization and practice. Our goal is to enhance privacy protections in ways that do not impede this evolution. For example, we received many comments asking us to assign a status under this regulation based on a label or title. For example, many commenters asked whether ''disease management'' is a ''health care operation,'' or whether a ''pharmacy benefits manager'' is a covered entity. From the comments and our fact-finding, however, we learned that these terms do not have consistent meanings today; rather, they encompass diverse activities and information practices. Further, the statutory definitions of key terms such as health care provider and health care clearinghouse describe functions, not specific types of persons or entities. To respect both the Congressional approach and industry evolution, we design the rule to follow activities and functions, not titles and labels.

Similarly, many comments asked whether a particular person would be a ''business associate'' under the rule, based on the nature of the person's business. Whether a business associate arrangement must exist under the rule, however, depends on the relationship between the entities and the services being performed, not on the type of persons or companies involved.

Our approach is also significantly informed by the limited jurisdiction conferred by HIPAA. In large part, we have the authority to regulate those who create and disclose health information, but not many key stakeholders who receive that health information from a covered entity. Again, this led us to look to the balance between the burden on covered entities and need to protect privacy in determining our approach to such disclosures. In some instances, we approach this dilemma by requiring covered entities to obtain a representation or documentation of purpose from the person requesting information. While there would be advantages to legislation regulating such third persons directly, we cannot justify abandoning any effort to enhance privacy.

It also became clear from the comments and our fact-finding that we have expectations as a society that conflict with individuals' views about the privacy of health information. We expect the health care industry to develop treatment protocols for the delivery of high quality health care. We expect insurers and the government to reduce fraud in the health care system. We expect to be protected from epidemics, and we expect medical research to produce miracles. We expect the police to apprehend suspects, and we expect to pay for our care by credit card. All of these activities involve disclosure of health information to someone other than our physician.

While most commenters support the concept of health privacy in general, many go on to describe activities that depend on the disclosure of health information and urge us to protect those information flows. Section III, in which we respond to the comments, describes our approach to balancing these conflicting expectations.

Finally, we note that many commenters were concerned that this regulation would lessen current privacy protections. It is important to understand this regulation as a new federal floor of privacy protections that does not disturb more protective rules or practices. Nor do we intend this regulation to describe a set of a ''best practices.'' Rather, this regulation describes a set of basic consumer protections and a series of regulatory permissions for use and disclosure of health information. The protections are a mandatory floor, which other governments and any covered entity may exceed. The permissions are just that, permissive—the only disclosures of health information required under this rule are to the individual who is the subject of the information or to the Secretary for enforcement of this rule. We expect covered entities to rely on their professional ethics and use their own best judgements in deciding which of these permissions they will use.

Combining Workability With New Protections

This rule establishes national minimum standards to protect the privacy of individually identifiable health information in prescribed

settings. The standards address the many varied uses and disclosures of individually identifiable health information by health plans, certain health care providers and health care clearinghouses. The complexity of the standards reflects the complexity of the health care marketplace to which they apply and the variety of subjects that must be addressed. The rule applies not only to the core health care functions relating to treating patients and reimbursing health care providers, but also to activities that range from when individually identifiable health information should be available for research without authorization to whether a health care provider may release protected health information about a patient for law enforcement purposes. The number of discrete provisions, and the number of commenters requesting that the rule recognize particular activities, is evidence of the significant role that individually identifiable health information plays in many vital public and private concerns.

At the same time, the large number of comments from individuals and groups representing individuals demonstrate the deep public concern about the need to protect the privacy of individually identifiable health information. The discussion above is rich with evidence about the importance of protecting privacy and the potential adverse consequences to individuals and their health if such protections are not extended.

The need to balance these competing interests—the necessity of protecting privacy and the public interest in using identifiable health information for vital public and private purposes—in a way that is also workable for the varied stakeholders causes much of the complexity in the rule. Achieving workability without sacrificing protection means some level of complexity, because the rule must track current practices and current practices are complex. We believe that the complexity entailed in reflecting those practices is better public policy than a perhaps simpler rule that disturbed important information flows.

Although the rule taken as a whole is complicated, we believe that the standards are much less complex as they apply to particular actors. What a health plan or covered health care provider must do to comply with the rule is clear, and the two-year delayed implementation provides a substantial period for trade and professional associations, working with their members, to assess the effects of the standards and develop policies and procedures to come into compliance with them. For individuals, the system may look substantially more complicated because, for the first time, we are ensuring that individuals will receive detailed information about how their individually identifiable health information may be used and disclosed. We also provide individuals with additional tools to exercise some control over those uses and disclosures. The additional complexity for individuals is the price of expanding their understanding and their rights.

The Department will work actively with members of the health care industry, representatives of individuals and others during the implementation of this rule. As stated elsewhere, our focus is to develop broader understanding of how the standards work and to facilitate compliance. We intend to provide guidance and check lists as appropriate, particularly to small businesses affected by the rule. We also will work with trade and professional associations to develop guidance and provide technical assistance so that they can help their members understand and comply with these new standards. If this effort is to succeed, the various public and private participants inside and outside of the health care system will need to work together to assure that the competing interests described above remain in balance and that an ethic that recognizes their importance is established.

Enforcement

The Secretary has decided to delegate her responsibility under this regulation to the Department's Office for Civil Rights (OCR). OCR will be responsible for enforcement of this regulation. Enforcement activities will include working with covered entities to secure voluntary compliance through the provision of technical assistance and other means; responding to questions regarding the regulation and providing interpretations and guidance; responding to state requests for exception determinations; investigating complaints and conducting compliance reviews; and, where voluntary compliance cannot be achieved, seeking civil monetary penalties and making referrals for criminal prosecution.

Consent

Current Law and Practice

The issue that drew the most comments overall is the question of when individuals' permission should be obtained prior to use or disclosure of their health information. We learned that individuals' views and the legal view of ''consent'' for use and disclosure of health information are different and in many ways incompatible. Comments from individuals revealed a common belief that, today, people must be asked permission for each and every release of their health information. Many believe that they ''own'' the health records about them. However, current law and practice do not support this view.

Current privacy protection practices are determined in part by the standards and practices that the professional associations have adopted for their members. Professional codes of conduct for ethical behavior generally can be found as opinions and guidelines developed by organizations such as the American Medical Association, American Nurses' Association, the American Hospital Association, the American Psychiatric Association, and the American Dental Association. These are generally issued though an organization's governing body. The codes do not have the force of law, but providers often recognize them as binding rules.

Our review of professional codes of ethics revealed partial, but loose, support for individuals' expectations of privacy. For example, the American Medical Association's Code of Ethics recognizes both the right to privacy and the need to balance it against societal needs. It reads in part: ''conflicts between a patient's right to privacy and a third party's need to know should be resolved in favor of the patient, except where that would result in serious health hazard or harm to the patient or others.'' AMA Policy No 140.989. See also, Mass. Med. Society, Patient Privacy and Confidentiality (1996), at 14:

> Patients enter treatment with the expectation that the information they share will be used exclusively for their clinical care. Protection of our patients' confidences is an integral part of our ethical training.

These codes, however, do not apply to many who obtain information from providers. For example, the National Association of Insurance Commissioners model code, ''Health Information Privacy Model Act'' (1998), applies to insurers but has not been widely adopted. Codes of ethics are also often written in general terms that do not provide guidance to providers and plans confronted with specific questions about protecting health information.

State laws are a crucial means of protecting health information, and today state laws vary dramatically. Some states defer to the professional codes of conduct, others provide general guidelines for privacy protection, and

others provide detailed requirements relating to the protection of information relating to specific diseases or to entire classes of information. Cf., D.C. Code Ann. § 2–3305.14(16) and Haw. Rev. Stat. 323C, *et seq.* In general, state statutes and case law addressing consent to use of health information do not support the public's strong expectations regarding consent for use and disclosure of health information. Only about half of the states have a general law that prohibits disclosure of health information without patient authorization and some of these are limited to hospital medical records.

Even when a state has a law limiting disclosure of health information, the law typically exempts many types of disclosure from the authorization requirement. Georgetown Study, Key Findings; Lisa Dahm, ''50-State Survey on Patient Health Care Record Confidentiality,'' American Health Lawyers Association (1999). One of the most common exemptions from a consent requirement is disclosure of health information for treatment and related purposes. See, *e.g.,* Wis.Stat. § 164.82; Cal. Civ. Code 56:10; National Conference of Commissioners on Uniform State Laws, *Uniform Health-Care Information Act, Minneapolis, MN, August 9, 1985.* Some states include utilization review and similar activities in the exemption. See, *e.g.,* Ariz. Rev. Stat. § 12–2294. Another common exemption from consent is disclosure of health information for purposes of obtaining payment. See, *e.g.,* Fla. Stat. Ann. § 455.667; Tex. Rev. Civ. Stat. Art. 4495, § 5.08(h); 410 Ill. Comp. Stat. 50/3(d). Other common exemptions include disclosures for emergency care, and for disclosures to government authorities (such as a department of public health). See Gostin Study, at 1–2; 48–51. Some states also exempt disclosure to law enforcement officials (*e.g.,* Massachusetts, Ch. 254 of the Acts of 2000), coroners (Wis. Stat. § 146.82), and for such purposes as business operations, oversight, research, and for directory information. Under these exceptions, providers can disclose health information without any consent or authorization from the patient. When states require specific, written authorization for disclosure of health information, the authorizations are usually only required for certain types of disclosures or certain types of information, and one authorization can suffice for multiple disclosures over time.

The states that do not have laws prohibiting disclosure of health information impose no specific requirements for consent or authorization prior to release of health information. There may, however, be other controls on release of health information. For instance, most health care professional licensure laws include general prohibitions against ''breaches of confidentiality.'' In some states, patients can hold providers accountable for some unauthorized disclosures of health information about them under various tort theories, such as invasion of privacy and breach of a confidential relationship. While these controls may affect certain disclosure practices, they do not amount to a requirement that a provider obtain authorization for each and every disclosure of health information.

Further, patients are typically not given a choice; they must sign the ''consent'' in order to receive care. As the Georgetown Study points out, ''In effect, the authorization may function more as a waiver of consent—the patient may not have an opportunity to object to any disclosures.'' Georgetown Study, Key Findings.

In the many cases where neither state law nor professional ethical standards exist, the only privacy protection individuals have is limited to the policies and procedures that the health care entity adopts. Corporate privacy policies are often proprietary. While several professional associations attached their privacy principles to their comments, health care entities did not. One study we found indicates that these policies are not adequate to provide appropriate privacy protections and alleviate public concern. The Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure made multiple findings highlighting the need for heightened privacy and security, including:

> Finding 5: The greatest concerns regarding the privacy of health information derives from widespread sharing of patient information throughout the health care industry and the inadequate federal and state regulatory framework for systematic protection of health information.
>
> *For the Record: Protecting Electronic Health Information*, National Academy Press, Washington DC, 1997.

Consent Under This Rule

In the NPRM, we expressed concern about the coercive nature of consents currently obtained by providers and plans relating to the use and disclosure of health information. We also expressed concern about the lack of information available to the patient during the process, and the fact that patients often were not even presented with a copy of the consent that they have signed. These and other concerns led us to propose that covered entities be permitted to use and disclose protected health information for treatment, payment and health care operations without the express consent of the subject individual.

In the final rule, we alter our proposed approach and require, in most instances, that health care providers who have a direct treatment relationship with their patients obtain the consent of their patients to use and disclose protected health information for treatment, payment and health care operations. While our concern about the coerced nature of these consents remains, many comments that we received from individuals, health care professionals, and organizations that represent them indicated that both patients and practitioners believe that patient consent is an important part of the current health care system and should be retained.

Providing and obtaining consent clearly has meaning for patients and practitioners. Patient advocates argued that the act of signing focuses the patient's attention on the substance of the transaction and provides an opportunity for the patient to ask questions about or seek modifications in the provider's practices. Many health care practitioners and their representatives argued that seeking a patient's consent to disclose confidential information is an ethical requirement that strengthens the physician-patient relationship. Both practitioners and patients argued that the approach proposed in the NPRM actually reduced patient protections by eliminating the opportunity for patients to agree to how their confidential information would be used and disclosed.

While we believe that the provisions in the NPRM that provided for detailed notice to the patient and the right to request restrictions would have provided an opportunity for patients and providers to discuss and negotiate over information practices, it is clear from the comments that many practitioners and patients believe the approach proposed in the NPRM is not an acceptable replacement for the patient providing consent.

To encourage a more informed interaction between the patient and the provider during the consent process, the final rule requires that the consent form that is presented to the patient be accompanied by a notice that contains a detailed discussion of the provider's health information practices. The consent form must reference the notice and also must inform the patient that he

or she has the right to ask the health care provider to request certain restrictions as to how the information of the patient will be used or disclosed. Our goal is to provide an opportunity for and to encourage more informed discussions between patients and providers about how protected health information will be used and disclosed within the health care system.

We considered and rejected other approaches to consent, including those that involved individuals providing a global consent to uses and disclosures when they sign up for insurance. While such approaches do require the patient to provide consent, it is not really an informed one or a voluntary one. It is also unclear how a consent obtained at the enrollment stage would be meaningfully communicated to the many providers who create the health information in the first instance. The ability to negotiate restrictions or otherwise have a meaningful discussion with the front-line provider would be independent of, and potentially in conflict with, the consent obtained at the enrollment stage. In addition, employers today are moving toward simplified enrollment forms, using check-off boxes and similar devices. The opportunity for any meaningful consideration or interaction at that point is slight. For these and other reasons, we decided that, to the extent a consent can accomplish the goal sought by individuals and providers, it must be focused on the direct interaction between an individual and provider.

The comments and fact-finding indicate that our approach will not significantly change the administrative aspect of consent as it exists today. Most direct treatment providers today obtain some type of consent for some uses and disclosures of health information. Our regulation will ensure that those consents cover the routine uses and disclosures of health information, and provide an opportunity for individuals to obtain further information and have further discussion, should they so desire.

Administrative Costs

Section 1172(b) of the Act provides that ''[a]ny standard adopted under this part [part C of title XI of the Act] shall be consistent with the objective of reducing the administrative costs of providing and paying for health care.'' The privacy and security standards are the platform on which the remaining standards rest; indeed, the design of part C of title XI makes clear that the various standards are intended to function together. Thus, the costs of privacy and security are properly attributable to the suite of administrative simplification regulations as a whole, and the cost savings realized should likewise be calculated on an aggregated basis, as is done below. Because the privacy standards are an integral and necessary part of the suite of Administrative Simplification standards, and because that suite of standards will result in substantial administrative cost savings, the privacy standards are ''consistent with the objective of reducing the administrative costs of providing and paying for health care.''

As more fully discussed in the Regulatory Impact and Regulatory Flexibility analyses below, we recognize that these privacy standards will entail substantial initial and ongoing administrative costs for entities subject to the rules. It is also the case that the privacy standards, like the security standards authorized by section 1173(d) of the Act, are necessitated by the technological advances in information exchange that the remaining Administrative Simplification standards facilitate for the health care industry. The same technological advances that make possible enormous administrative cost savings for the industry as a whole have also made it possible to breach the security and privacy of health information on a scale that was previously inconceivable. The Congress recognized that adequate protection of the security and privacy of health information is a *sine qua non* of the increased efficiency of information exchange brought about by the electronic revolution, by enacting the security and privacy provisions of the law. Thus, as a matter of policy as well as law, the administrative standards should be viewed as a whole in determining whether they are ''consistent with'' the objective of reducing administrative costs.

Consultations

The Congress required the Secretary to consult with specified groups in developing the standards under sections 262 and 264. Section 264(d) of HIPAA specifically requires the Secretary to consult with the National Committee on Vital and Health Statistics (NCVHS) and the Attorney General in carrying out her responsibilities under the section. Section 1172(b)(3) of the Act, which was enacted by section 262, requires that, in developing a standard under section 1172 for which no standard setting organization has already developed a standard, the Secretary must, before adopting the standard, consult with the National Uniform Billing Committee (NUBC), the National Uniform Claim Committee (NUCC), the Workgroup for Electronic Data Interchange (WEDI), and the American Dental Association (ADA). Section 1172(f) also requires the Secretary to rely on the recommendations of the NCVHS and consult with other appropriate federal and state agencies and private organizations.

We engaged in the required consultations including the Attorney General, NUBC, NUCC, WEDI and the ADA. We consulted with the NCVHS in developing the Recommendations, upon which this proposed rule is based. We continued to consult with this committee by requesting the committee to review the proposed rule and provide comments prior to its publication, and by reviewing transcripts of its public meeting on privacy and related topics. We consulted with representatives of the National Congress of American Indians, the National Indian Health Board, and the self governance tribes. We also met with representatives of the National Governors' Association, the National Conference of State Legislatures, the National Association of Public Health Statistics and Information Systems, and a number of other state organizations to discuss the framework for the proposed rule, issues of special interests to the states, and the process for providing comments on the proposed rule.

Many of these groups submitted comments to the proposed rule, and those were taken into account in developing the final regulation.

In addition to the required consultations, we met with numerous individuals, entities, and agencies regarding the regulation, with the goal of making these standards as compatible as possible with current business practices, while still enhancing privacy protection. During the open comment period, we met with dozens of groups.

Relevant federal agencies participated in the interagency working groups that developed the NPRM and the final regulation, with additional representatives from all operating divisions and many staff offices of HHS. The following federal agencies and offices were represented on the interagency working groups: the Department of Justice, the Department of Commerce, the Social Security Administration, the Department of Defense, the Department of Veterans Affairs, the Department of Labor, the Office of Personnel Management, and the Office of Management and Budget.

II. Section-by-Section Description of Rule Provisions

Part 160—Subpart A—General Provisions

Part 160 applies to all the administrative simplification regulations. We include the entire regulation text in this rule, not just those provisions relevant to this Privacy regulation. For example, the term ''trading partner'' is defined here, for use in the Health Insurance Reform: Standards for Electronic Transactions regulation, published at 65 FR 50312, August 17, 2000 (the ''Transactions Rule''). It does not appear in the remainder of this Privacy rule.

Sections 160.101 and 160.104 of Subpart A of part 160 were promulgated in the Transactions Rule, and we do not change them here. We do, however, make changes and additions to § 160.103, the definitions section of Subpart A. The definitions that were promulgated in the Transactions Rule and that remain unchanged here are: Act, ANSI, covered entity, compliance date, group health plan, HCFA, HHS, health care provider, health information, health insurance issuer, health maintenance organization, modify or modification, Secretary, small health plan, standard setting organization, and trading partner agreement. Of these terms, we discuss further in this preamble only covered entity and health care provider.

Section 160.102—Applicability

The proposed rule stated that the subchapter (Parts 160, 162, and 164) applies to the entities set out at section 1172(a) of the Act: Health plans, health care clearinghouses, and health care providers who transmit any health information in electronic form in connection with a transaction covered by the subchapter. The final rule adds a provision (§ 160.102(b)) clarifying that to the extent required under section 201(a)(5) of HIPAA, nothing in the subchapter is to be construed to diminish the authority of any Inspector General. This was done in response to comment, to clarify that the administrative simplification rules, including the rules below, do not conflict with the cited provision of HIPAA.

Section 160.103—Definitions

Business Associate

We proposed to define the term ''business partner'' to mean, with respect to a covered entity, a person to whom the covered entity discloses protected health information so that the person can carry out, assist with the performance of, or perform on behalf of, a function or activity for the covered entity. ''Business partner'' would have included contractors or other persons who receive protected health information from the covered entity (or from another business partner of the covered entity) for the purposes described in the previous sentence, including lawyers, auditors, consultants, third-party administrators, health care clearinghouses, data processing firms, billing firms, and other covered entities. ''Business partner'' would have excluded persons who are within the covered entity's workforce, as defined in this section.

This rule reflects the change in the name from ''business partner'' to ''business associate,'' included in the Transactions Rule.

In the final rule, we change the definition of ''business associate'' to clarify the circumstances in which a person is acting as a business associate of a covered entity. The changes clarify that the business association occurs when the right to use or disclose the protected health information belongs to the covered entity, and another person is using or disclosing the protected health information (or creating, obtaining and using the protected health information) to perform a function or activity on behalf of the covered entity. We also clarify that providing specified services to a covered entity creates a business associate relationship if the provision of the service involves the disclosure of protected health information to the service provider. In the proposed rule, we had included a list of persons that were considered to be business partners of the covered entity. However, it is not always clear whether the provision of certain services to a covered entity is ''for'' the covered entity or whether the service provider is acting ''on behalf of'' the covered entity. For example, a person providing management consulting services may need protected health information to perform those services, but may not be acting ''on behalf of'' the covered entity. This we believe led to some general confusion among the commenters as to whether certain arrangements fell within the definition of a business partner under the proposed rule. The construction of the final rule clarifies that the provision of the specified services gives rise to a business associate relationship if the performance of the service involves disclosure of protected health information by the covered entity to the business associate. The specified services are legal, actuarial, accounting, consulting, management, administrative accreditation, data aggregation, and financial services. The list is intended to include the types of services commonly provided to covered entities where the disclosure of protected health information is routine to the performance of the service, but when the person providing the service may not always be acting ''on behalf of'' the covered entity.

In the final rule, we reorganize the list of examples of the functions or activities that may be conducted by business associates. We place a part of the proposed list in the portion of the definition that addresses when a person is providing functions or activities for or on behalf of a covered entity. We place other parts of the list in the portion of the definition that specifies the services that give rise to a business associate relationship, as discussed above. We also have expanded the examples to provide additional guidance and in response to questions from commenters.

We have added data aggregation to the list of services that give rise to a business associate relationship. Data aggregation, as discussed below, is where a business associate in its capacity as the business associate of one covered entity combines the protected health information of such covered entity with protected health information received by the business associate in its capacity as a business associate of another covered entity in order to permit the creation of data for analyses that relate to the health care operations of the respective covered entities. Adding this service to the business associate definition clarifies the ability of covered entities to contract with business associates to undertake quality assurance and comparative analyses that involve the protected health information of more than one contracting covered entity. For example, a state hospital association could act as a business associate of its member hospitals and could combine data provided to it to assist the hospitals in evaluating their relative performance in areas such as quality, efficiency and other patient care issues. As discussed below, however, the business associate contracts of each of the hospitals would have to permit the activity, and the protected health information of one hospital could not be disclosed to another hospital unless the disclosure is otherwise permitted by the rule.

The definition also states that a business associate may be a covered entity, and that business associate excludes a person who is part of the covered entity's workforce.

We also clarify in the final rule that a business association arises with

respect to a covered entity when a person performs functions or activities on behalf of, or provides the specified services to or for, an organized health care health care arrangement in which the covered entity participates. This change recognizes that where covered entities participate in certain joint arrangements for the financing or delivery of health care, they often contract with persons to perform functions or to provide services for the joint arrangement. This change is consistent with changes made in the final rule to the definition of health care operations, which permits covered entities to use or disclose protected health information not only for their own health care operations, but also for the operations of an organized health care arrangement in which the covered entity participates. By making these changes, we avoid the confusion that could arise in trying to determine whether a function or activity is being provided on behalf of (or if a specified service is being provided to or for) a covered entity or on behalf of or for a joint enterprise involving the covered entity. The change clarifies that in either instance the person performing the function or activity (or providing the specified service) is a business associate.

We also add language to the final rule that clarifies that the mere fact that two covered entities participate in an organized health care arrangement does not make either of the covered entities a business associate of the other covered entity. The fact that the entities participate in joint health care operations or other joint activities, or pursue common goals through a joint activity, does not mean that one party is performing a function or activity on behalf of the other party (or is providing a specified services to or for the other party).

In general under this provision, actions relating to the protected health information of an individual undertaken by a business associate are considered, for the purposes of this rule, to be actions of the covered entity, although the covered entity is subject to sanctions under this rule only if it has knowledge of the wrongful activity and fails to take the required actions to address the wrongdoing. For example, if a business associate maintains the medical records or manages the claims system of a covered entity, the covered entity is considered to have protected health information and the covered entity must ensure that individuals who are the subject of the information can have access to it pursuant to § 164.524.

The business associate relationship does not describe all relationships between covered entities and other persons or organizations. While we permit uses or disclosures of protected health information for a variety of purposes, business associate contracts or other arrangements are only required for those cases in which the covered entity is disclosing information to someone or some organization that will use the information on behalf of the covered entity, when the other person will be creating or obtaining protected health information on behalf of the covered entity, or when the business associate is providing the specified services to the covered entity and the provision of those services involves the disclosure of protected health information by the covered entity to the business associate. For example, when a health care provider discloses protected health information to health plans for payment purposes, no business associate relationship is established. While the covered provider may have an agreement to accept discounted fees as reimbursement for services provided to health plan members, neither entity is acting on behalf of or providing a service to the other.

Similarly, where a physician or other provider has staff privileges at an institution, neither party to the relationship is a business associate based solely on the staff privileges because neither party is providing functions or activities on behalf of the other. However, if a party provides services to or for the other, such as where a hospital provides billing services for physicians with staff privileges, a business associate relationship may arise with respect to those services. Likewise, where a group health plan purchases insurance or coverage from a health insurance issuer or HMO, the provision of insurance by the health insurance issuer or HMO to the group health plan does not make the issuer a business associate. In such case, the activities of the health insurance issuer or HMO are on their own behalf and not on the behalf of the group health plan. We note that where a group health plan contracts with a health insurance issuer or HMO to perform functions or activities or to provide services that are in addition to or not directly related to the provision of insurance, the health insurance issuer or HMO may be a business associate with respect to those additional functions, activities or services. We also note that covered entities are permitted to disclose protected health information to oversight agencies that act to provide oversight of federal programs and the health care system. These oversight agencies are not performing services for or on behalf of the covered entities and so are not business associates of the covered entities. Therefore HCFA, the federal agency that administers Medicare, is not required to enter into a business associate contract in order to disclose protected health information to the Department's Office of Inspector General.

We do not require a covered entity to enter into a business associate contract with a person or organization that acts merely as a conduit for protected health information (*e.g.,* the US Postal Service, certain private couriers and their electronic equivalents). A conduit transports information but does not access it other than on a random or infrequent basis as may be necessary for the performance of the transportation service, or as required by law. Since no disclosure is intended by the covered entity and the probability of exposure of any particular protected health information to a conduit is very small, we do not consider a conduit to be a business associate of the covered entity.

We do not consider a financial institution to be acting on behalf of a covered entity, and therefore no business associate contract is required, when it processes consumer-conducted financial transactions by debit, credit or other payment card, clears checks, initiates or processes electronic funds transfers, or conducts any other activity that directly facilitates or effects the transfer of funds for compensation for health care. A typical consumer-conducted payment transaction is when a consumer pays for health care or health insurance premiums using a check or credit card. In these cases the identity of the consumer is always included and some health information (e.g., diagnosis or procedure) may be implied through the name of the health care provider or health plan being paid. Covered entities that initiate such payment activities must meet the minimum necessary disclosure requirements described in the preamble to § 164.514.

Covered Entity

We provided this definition in the NPRM for convenience of reference and proposed it to mean the entities to which part C of title XI of the Act applies. These are the entities described in section 1172(a)(1): Health plans, health care clearinghouses, and health care providers who transmit any health information in electronic form in connection with a transaction referred

to in section 1173(a)(1) of the Act (a ''standard transaction'').

We note that health care providers who do not submit HIPAA transactions in standard form become covered by this rule when other entities, such as a billing service or a hospital, transmit standard electronic transactions on their behalf. A provider could not circumvent these requirements by assigning the task to its business associate since the business associate would be considered to be acting on behalf of the provider. See the definition of ''business associate.''

Where a public agency is required or authorized by law to administer a health plan jointly with another entity, we consider each agency to be a covered entity with respect to the health plan functions it performs. Unlike private sector health plans, public plans are often required by or expressly authorized by law to jointly administer health programs that meet the definition of ''health plan'' under this regulation. In some instances the public entity is required or authorized to administer the program with another public agency. In other instances, the public entity is required or authorized to administer the program with a private entity. In either circumstance, we note that joint administration does not meet the definition of ''business associate'' in § 164.501. Examples of joint administration include state and federal administration of the Medicaid and SCHIP program, or joint administration of a Medicare+Choice plan by the Health Care Financing Administration and the issuer offering the plan.

Health Care

We proposed to define ''health care'' to mean the provision of care, services, or supplies to a patient and to include any: (1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, counseling, service, or procedure with respect to the physical or mental condition, or functional status, of a patient or affecting the structure or function of the body; (2) sale or dispensing of a drug, device, equipment, or other item pursuant to a prescription; or (3) procurement or banking of blood, sperm, organs, or any other tissue for administration to patients.

The final rule revises both the NPRM definition and the definition as provided in the Transactions Rule, to now mean ''care, services, or supplies related to the health of an individual. Health care includes the following:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and

(2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

We delete the term ''providing'' from the definition to delineate more clearly the relationship between ''treatment,'' as the term is defined in § 164.501, and ''health care.'' Other key revisions include adding the term ''assessment'' in subparagraph (1) and deleting proposed subparagraph (3) from the rule. Therefore the procurement or banking of organs, blood (including autologous blood), sperm, eyes or any other tissue or human product is not considered to be health care under this rule and the organizations that perform such activities would not be considered health care providers when conducting these functions. As described in § 164.512(h), covered entities are permitted to disclose protected health information without individual authorization, consent, or agreement (see below for explanation of authorizations, consents, and agreements) as necessary to facilitate cadaveric donation.

Health Care Clearinghouse

In the NPRM, we defined ''health care clearinghouse'' as a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements. The entity receives health care transactions from health care providers or other entities, translates the data from a given format into one acceptable to the intended payor or payors, and forwards the processed transaction to appropriate payors and clearinghouses. Billing services, repricing companies, community health management information systems, community health information systems, and ''value-added'' networks and switches would have been considered to be health care clearinghouses for purposes of this part, if they perform the functions of health care clearinghouses as described in the preceding sentences.

In the final regulation, we modify the definition of health care clearinghouse to reflect changes in the definition published in the Transactions Rule. The definition in the final rule is:

Health care clearinghouse means a public or private entity, including billing services, repricing companies, community health management information systems or community health information systems, and ''value-added'' networks and switches, that does either of the following functions:

(1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

(2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

We note here that the term health care clearinghouse may have other meanings and connotations in other contexts, but the regulation defines it specifically, and an entity is considered a health care clearinghouse only to the extent that it meets the criteria in this definition. Telecommunications entities that provide connectivity or mechanisms to convey information, such as telephone companies and Internet Service Providers, are not health care clearinghouses as defined in the rule unless they actually carry out the functions outlined in our definition. Value added networks and switches are not health care clearinghouses unless they carry out the functions outlined in the definition. The examples of entities in our proposed definition we continue to consider to be health care clearinghouses, as well as any other entities that meet that definition, to the extent that they perform the functions in the definition.

In order to fall within this definition of clearinghouse, the covered entity must perform the clearinghouse function on health information received from some other entity. A department or component of a health plan or health care provider that transforms nonstandard information into standard data elements or standard transactions (or vice versa) is not a clearinghouse for purposes of this rule, unless it also performs these functions for another entity. As described in more detail in § 164.504(d), we allow affiliates to perform clearinghouse functions for each other without triggering the definition of ''clearinghouse'' if the conditions in § 164.504(d) are met.

Health Care Provider

We proposed to define health care provider to mean a provider of services as defined in section 1861(u) of the Act, a provider of medical or health services as defined in section 1861(s) of the Act, and any other person or organization who furnishes, bills, or is paid for health care services or supplies in the normal course of business.

In the final rule, we delete the term ''services and supplies,'' in order to eliminate redundancy within the definition. The definition also reflects the addition of the applicable U.S.C. citations (42 U.S.C. 1395x(u) and 42 U.S.C. 1395x(s), respectively) for the referenced provisions of the Act that were promulgated in the Transactions Rule.

To assist the reader, we also provide here excerpts from the relevant sections of the Act. (Refer to the U.S.C. sections cited above for complete definitions in sections 1861(u) and 1861(s).) Section 1861(u) of the Act defines a ''provider of services,'' to include, for example,

a hospital, critical access hospital, skilled nursing facility, comprehensive outpatient rehabilitation facility, home health agency, hospice program, or, for purposes of section 1814(g) (42 U.S.C. 1395f(g)) and section 1835(e) (42 U.S.C. 1395n(e)), a fund.'' Section 1861(s) of the Act defines the term, ''medical and other health services,'' and includes a list of covered items or services, as illustrated by the following excerpt:

(s) Medical and other health services. The term ''medical and other health services'' means any of the following items or services:

(1) Physicians' services;

(2) (A) services and supplies * * * furnished as an incident to a physician's professional service, or kinds which are commonly furnished in physicians' offices and are commonly either rendered without charge or included in the physicians' bills;

(B) hospital services * * * incident to physicians' services rendered to outpatients and partial hospitalization services incident to such services;

(C) diagnostic services which are—

(i) furnished to an individual as an outpatient by a hospital or by others under arrangements with them made by a hospital, and

(ii) ordinarily furnished by such hospital (or by others under such arrangements) to its outpatients for the purpose of diagnostic study;

(D) outpatient physical therapy services and outpatient occupational therapy services;

(E) rural health clinic services and federally qualified health center services;

(F) home dialysis supplies and equipment, self-care home dialysis support services, and institutional dialysis services and supplies;

(G) antigens * * * prepared by a physician * * * for a particular patient, including antigens so prepared which are forwarded to another qualified person * * * for administration to such patient, * * * by or under the supervision of another such physician;

(H)(i) services furnished pursuant to a contract under section 1876 (42 U.S.C. 1395mm) to a member of an eligible organization by a physician assistant or by a nurse practitioner * * * and such services and supplies furnished as an incident to his service to such a member * * * and

(ii) services furnished pursuant to a risk-sharing contract under section 1876(g) (42 U.S.C. 1395mm(g)) to a member of an eligible organization by a clinical psychologist * * * or by a clinical social worker * * * (and) furnished as an incident to such clinical psychologist's services or clinical social worker's services * * *;

(I) blood clotting factors, for hemophilia patients * * *;

(J) prescription drugs used in immunosuppressive therapy furnished, to an individual who receives an organ transplant for which payment is made under this title (42 U.S.C. 1395 et seq.), but only in the case of (certain) drugs furnished * * *

(K)(i) services which would be physicians' services if furnished by a physician * * * and which are performed by a physician assistant * * *; and

(ii) services which would be physicians' services if furnished by a physician * * * and which are performed by a nurse * * *;

(L) certified nurse-midwife services;

(M) qualified psychologist services;

(N) clinical social worker services * * *;

(O) erythropoietin for dialysis patients * * *;

(P) prostate cancer screening tests * * *;

(Q) an oral drug (which is approved by the Federal Food and Drug Administration) prescribed for use as an anti-cancer chemotherapeutic agent for a given indication, and containing an active ingredient (or ingredients) * * *;

(R) colorectal cancer screening tests * * *;

(S) diabetes outpatient self-management training services * * *; and

(T) an oral drug (which is approved by the federal Food and Drug Administration) prescribed for use as an acute anti-emetic used as part of an anti-cancer chemotherapeutic regimen * * *

(3) diagnostic X-ray tests * * * furnished in a place of residence used as the patient's home * * * ;

(4) X-ray, radium, and radioactive isotope therapy, including materials and services of technicians;

(5) surgical dressings, and splints, casts, and other devices used for reduction of fractures and dislocations;

(6) durable medical equipment;

(7) ambulance service where the use of other methods of transportation is contraindicated by the individual's condition * * * ;

(8) prosthetic devices (other than dental) which replace all or part of an internal body organ (including colostomy bags and supplies directly related to colostomy care), * * * and including one pair of conventional eyeglasses or contact lenses furnished subsequent to each cataract surgery * * * [;]

(9) leg, arm, back, and neck braces, and artificial legs, arms, and eyes, including replacements if required * * * ;

(10) (A) pneumococcal vaccine and its administration * * *; and

(B) hepatitis B vaccine and its administration * * *, and

(11) services of a certified registered nurse anesthetist * * *;

(12) * * * extra-depth shoes with inserts or custom molded shoes with inserts for an individual with diabetes, if * * *;

(13) screening mammography * * *;

(14) screening pap smear and screening pelvic exam; and

(15) bone mass measurement * * *. (etc.)

Health Plan

We proposed to define ''health plan'' essentially as section 1171(5) of the Act defines it. Section 1171 of the Act refers to several definitions in section 2791 of the Public Health Service Act, 42 U.S.C. 300gg–91, as added by Public Law 104–191.

As defined in section 1171(5), a ''health plan'' is an individual plan or group health plan that provides, or pays the cost of, medical care. We proposed that this definition include, but not be limited to the 15 types of plans (*e.g.,* group health plan, health insurance issuer, health maintenance organization) listed in the statute, as well as any combination of them. Such term would have included, when applied to public benefit programs, the component of the government agency that administers the program. Church plans and government plans would have been included to the extent that they fall into one or more of the listed categories.

In the proposed rule, ''health plan'' included the following, singly or in combination:

(1) A group health plan, defined as an employee welfare benefit plan (as currently defined in section 3(1) of the Employee Retirement Income and Security Act of 1974, 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act, 42 U.S.C. 300gg–91(a)(2)), including items and services paid for as medical care, to employees or their dependents directly or through insurance or otherwise, that:

(i) Has 50 or more participants; or

(ii) Is administered by an entity other than the employer that established and maintains the plan.

(2) A health insurance issuer, defined as an insurance company, insurance service, or insurance organization that is licensed to engage in the business of insurance in a state and is subject to state or other law that regulates insurance.

(3) A health maintenance organization, defined as a federally qualified health maintenance organization, an organization recognized as a health maintenance organization under state law, or a similar organization regulated for solvency under state law in the same manner and to the same extent as such a health maintenance organization.

(4) Part A or Part B of the Medicare program under title XVIII of the Act.

(5) The Medicaid program under title XIX of the Act.

(6) A Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss).

(7) A long-term care policy, including a nursing home fixed-indemnity policy.

(8) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.

(9) The health care program for active military personnel under title 10 of the United States Code.

(10) The veterans health care program under 38 U.S.C. chapter 17.

(11) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS), as defined in 10 U.S.C. 1072(4).

(12) The Indian Health Service program under the Indian Health Care Improvement Act (25 U.S.C. 1601, *et seq.*).

(13) The Federal Employees Health Benefits Program under 5 U.S.C. chapter 89.

(14) An approved state child health plan for child health assistance that meets the requirements of section 2103 of the Act.

(15) A Medicare Plus Choice organization as defined in 42 CFR 422.2, with a contract under 42 CFR part 422, subpart K.

In addition to the 15 specific categories, we proposed that the list include any other individual plan or group health plan, or combination thereof, that provides or pays for the cost of medical care. The Secretary would determine which plans that meet these criteria would to be considered health plans for the purposes of this rule.

Consistent with the other titles of HIPAA, our proposed definition did not include certain types of insurance entities, such as workers' compensation and automobile insurance carriers, other property and casualty insurers, and certain forms of limited benefits coverage, even when such arrangements provide coverage for health care services.

In the final rule, we add two provisions to clarify the types of policies or programs that we do not consider to be a health plan. First, the rule excepts any policy, plan or program to the extent that it provides, or pays for the cost of, excepted benefits, as defined in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg–91(c)(1). We note that, while coverage for on-site medical clinics is excluded from definition of ''health plans,'' such clinics may meet the definition of ''health care provider'' and persons who work in the clinic may also meet the definition of health care provider.'' Second, many commenters were confused by the statutory inclusion as a health plan of any ''other individual or group plan that provides or pays the cost of medical care;'' they questioned how the provision applied to many government programs. We therefore clarify that while many government programs (other than the programs specified in the statute) provide or pay the cost of medical care, we do not consider them to be individual or group plans and therefore, do not consider them to be health plans. Government funded programs that do not have as their principal purpose the provision of, or payment for, the cost of health care but which do incidentally provide such services are not health plans (for example, programs such as the Special Supplemental Nutrition Program for Women, Infants and Children (WIC) and the Food Stamp Program, which provide or pay for nutritional services, are not considered to be health plans). Government funded programs that have as their principal purpose the provision of health care, either directly or by grant, are also not considered to be health plans. Examples include the Ryan White Comprehensive AIDS Resources Emergency Act, government funded health centers and immunization programs. We note that some of these may meet the rule's definition of health care provider.

We note that in certain instances eligibility for or enrollment in a health plan that is a government program providing public benefits, such as Medicaid or SCHIP, is determined by an agency other than the agency that administers the program, or individually identifiable health information used to determine enrollment or eligibility in such a health plan is collected by an agency other than the agency that administers the health plan. In these cases, we do not consider an agency that is not otherwise a covered entity, such as a local welfare agency, to be a covered entity because it determines eligibility or enrollment or collects enrollment information as authorized by law. We also do not consider the agency to be a business associate when conducting these functions, as we describe further in the business associate discussion above.

The definition in the final rule also reflects the following changes promulgated in the Transactions Rule:

(1) Exclusion of nursing home fixed-indemnity policies;

(2) Addition of the word ''issuer'' to Medicare supplemental policy, and long-term care policy;

(3) Addition or revision of the relevant statutory cites where appropriate;

(4) Deletion of the term ''or assisted'' when referring to government programs;

(5) Replacement of the word ''organization'' with ''program'' when referring to Medicare + Choice;

(6) Deletion of the term ''health'' when referring to a group plan in subparagraph (xvi);

(7) Extraction of the definitions of ''group health plan,'' ''health insurance issuer,'' and ''health maintenance organization'' into Part 160 as distinct definitions;

(8) In the definition of ''group health plan,'' deletion of the term ''currently'' from the reference to the statutory cite of ERISA, addition of the relevant statutory cite for the term ''participant,'' and addition of the term ''reimbursement;''

(9) In the definition of ''health insurance issuer,'' addition of the relevant statutory cite, deletion of the term ''or other law'' after ''state law,'' addition of health maintenance organizations for consistency with the statute, and clarification that the term does not include a group health plan; and

(10) In the definition of ''health maintenance organization,'' addition of the relevant statutory cite.

Finally, we add to this definition a high risk pool that is a mechanism established under state law to provide health insurance coverage or comparable coverage to eligible individuals. High risk pools are designed mainly to provide health insurance coverage for individuals who, due to health status or pre-existing conditions, cannot obtain insurance through the individual market or who can do so only at very high premiums. Some states use their high risk pool as an alternative mechanism under section 2744 of HIPAA. We do not reference the definition of ''qualified high risk pool'' in HIPAA because that definition includes the requirements for a state to use its risk pool as its alternative mechanism under HIPAA. Some states may have high risk pools, but do not use them as their alternative mechanism and therefore may not meet the definition in HIPAA. We want to make clear that state high risk pools are covered entities under this rule whether or not they meet the definition of a qualified high risk pool under section 2744. High risk pools, as described in this rule, do not include any program established under state law solely to provide excepted benefits. For example, a state program established to provide workers' compensation coverage is not

considered to be a high risk pool under the rule.

Implementation Specification

This definition was adopted in the Transactions Rule and is minimally revised here. We add the words ''requirements or'' before the word ''instructions.'' The word ''instructions'' is appropriate in the context of the implementation specifications adopted in the Transactions Rule, which are generally a series of instructions as to how to use particular electronic forms. However, that word is not apropos in the context of the rules below. In the rules below, the implementation specifications are specific requirements for how to comply with a given standard. The change to this definition thus ties in to this regulatory framework.

Standard

This definition was adopted in the Transactions Rule and we have modified it to make it clearer. We also add language reflecting section 264 of the statute, to clarify that the standards adopted by this rule meet this definition.

State

We modify the definition of state as adopted in the Transactions Rule to clarify that this term refers to any of the several states.

Transaction

We change the term ''exchange'' to the term ''transmission'' in the definition of Transaction to clarify that these transactions may be one-way communications.

Workforce

We proposed in the NPRM to define workforce to mean employees, volunteers, trainees, and other persons under the direct control of a covered entity, including persons providing labor on an unpaid basis.

The definition in the final rule reflects one revision established in the Transactions Rule, which replaces the term ''including persons providing labor on an unpaid basis'' with the term ''whether or not they are paid by the covered entity.'' In addition, we clarify that if the assigned work station of persons under contract is on the covered entity's premises and such persons perform a substantial proportion of their activities at that location, the covered entity may choose to treat them either as business associates or as part of the workforce, as explained in the discussion of the definition of business associate. If there is no business associate contract, we assume the person is a member of the covered entity's workforce. We note that independent contractors may or may not be workforce members. However, for compliance purposes we will assume that such personnel are members of the workforce if no business associate contract exists.

Part 160—Subpart B—Preemption of State Laws

Statutory Background

Section 1178 of the Act establishes a ''general rule'' that state law provisions that are contrary to the provisions or requirements of part C of title XI or the standards or implementation specifications adopted or established thereunder are preempted by the federal requirements. The statute provides three exceptions to this general rule: (1) In section 1178(a)(2)(A)(i), for state laws that the Secretary determines are necessary to prevent fraud and abuse, ensure appropriate state regulation of insurance and health plans, for state reporting on health care delivery, and other purposes; (2) in section 1178(a)(2)(A)(ii), for state laws that address controlled substances; and (3) in section 1178(a)(2)(B), for state laws relating to the privacy of individually identifiable health information that as provided for by the related provision of section 264(c)(2) of HIPAA, are contrary to and more stringent than the federal requirements. Section 1178 also carves out, in sections 1178(b) and 1178(c), certain areas of state authority that are not limited or invalidated by the provisions of part C of title XI: these areas relate to public health and state regulation of health plans.

The NPRM proposed a new Subpart B of the proposed part 160. The new Subpart B, which would apply to all standards, implementation specifications, and requirements adopted under HIPAA, would consist of four sections. Proposed § 160.201 provided that the provisions of Subpart B applied to exception determinations and advisory opinions issued by the Secretary under section 1178. Proposed § 160.202 set out proposed definitions for four terms: (1) ''Contrary,'' (2) ''more stringent,'' (3) ''relates to the privacy of individually identifiable health information,'' and (4) ''state law.'' The definition of ''contrary'' was drawn from case law concerning preemption. A seven-part set of specific criteria, drawn from fair information principles, was proposed for the definition of ''more stringent.'' The definition of ''relates to the privacy of individually identifiable health information'' was also based on case law. The definition of ''state law'' was drawn from the statutory definition of this term elsewhere in HIPAA. We note that state action having the force and effect of law may include common law. We eliminate the term ''decision'' from the proposed rule because it is redundant.

Proposed § 160.203 proposed a general rule reflecting the statutory general rule and exceptions that generally mirrored the statutory language of the exceptions. The one substantive addition to the statutory exception language was with respect to the statutory exception, ''for other purposes.'' The following language was added: ''for other purposes related to improving the Medicare program, the Medicaid program, or the efficiency and effectiveness of the health care system.''

Proposed § 160.204 proposed two processes, one for the making of exception determinations, relating to determinations under section 1178(a)(2)(A) of the Act, the other for the rendering of advisory opinions, with respect to section 1178(a)(2)(B) of the Act. The processes proposed were similar in the following respects: (1) Only the state could request an exception determination or advisory opinion, as applicable; (2) both required the request to contain the same information, except that a request for an exception determination also had to set out the length of time the requested exception would be in effect, if less than three years; (3) both sets of requirements provided that requests had to be submitted to the Secretary as required by the Secretary, and until the Secretary's determination was made, the federal standard, requirement or implementation specification remained in effect; (4) both sets of requirements provided that the Secretary's decision would be effective intrastate only; (5) both sets of requirements provided that any change to either the federal or state basis for the Secretary's decision would require a new request, and the federal standard, implementation specification, or requirement would remain in effect until the Secretary acted favorably on the new request; (6) both sets of requirements provided that the Secretary could seek changes to the federal rules or urge states or other organizations to seek changes; and (7) both sets of requirements provided for annual publication of Secretarial decisions. In addition, the process for exception determinations provided for a maximum effective period of three years for such determinations.

The following changes have been made to subpart B in the final rules. First, § 160.201 now expressly

implements section 1178. Second, the definition of ''more stringent'' has been changed by eliminating the criterion relating to penalties and by framing the criterion under paragraph (1) more generally. Also, we have clarified that the term ''individual'' means the person who is the subject of the individually identifiable health information, since the term ''individual'' is defined this way only in subpart E of part 164, not in part 160. Third, the definition of ''state law'' has been changed by substituting the words ''statute, constitutional provision'' for the word ''law,'' the words ''common law'' for the word ''decision,'' and adding the words ''force and'' before the word ''effect'' in the proposed definition. Fourth, in § 160.203, several criteria relating to the statutory grounds for exception determinations have been further spelled out: (1) The words '' related to the provision of or payment for health care'' have been added to the exception for fraud and abuse; (2) the words ''to the extent expressly authorized by statute or regulation'' have been added to the exception for state regulation of health plans; (3) the words ''of serving a compelling need related to public health, safety, or welfare, and, where a standard, requirement, or implementation specification under part 164 of this subchapter is at issue, where the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served'' have been added to the general exception ''for other purposes''; and (4) the statutory provision regarding controlled substances has been elaborated on as follows: ''Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substance, as defined at 21 U.S.C. 802, or which is deemed a controlled substance by state law.''

The most extensive changes have been made to proposed § 160.204. The provision for advisory opinions has been eliminated. Section 160.204 now sets out only a process for requesting exception determinations. In most respects, this process is the same as proposed. However, the proposed restriction of the effect of exception determinations to wholly intrastate transactions has been eliminated. Section 160.204(a) has been modified to allow any person, not just a state, to submit a request for an exception determination, and clarifies that requests from states may be made by the state's chief elected official or his or her designee. Proposed § 160.204(a)(3) stated that if it is determined that the federal standard, requirement, or implementation specification in question meets the exception criteria as well as or better than the state law for which the exception is requested, the request will be denied; this language has been deleted. Thus, the criterion for granting or denying an exception request is whether the applicable exception criterion or criteria are met.

A new § 160.205 is also adopted, replacing part of what was proposed at proposed § 160.204. The new § 160.205 sets out the rules relating to the effectiveness of exception determinations. Exception determinations are effective until either the underlying federal or state laws change or the exception is revoked, by the Secretary, based on a determination that the grounds supporting the exception no longer exist. The proposed maximum of three years has been eliminated.

Relationship to Other Federal Laws

Covered entities subject to these rules are also subject to other federal statutes and regulations. For example, federal programs must comply with the statutes and regulations that govern them. Pursuant to their contracts, Medicare providers must comply with the requirements of the Privacy Act of 1974. Substance abuse treatment facilities are subject to the Substance Abuse Confidentiality provisions of the Public Health Service Act, section 543 and its regulations. And, health care providers in schools, colleges, and universities may come within the purview of the Family Educational Rights and Privacy Act. Thus, covered entities will need to determine how the privacy regulation will affect their ability to comply with these other federal laws.

Many commenters raised questions about how different federal statutes and regulations intersect with the privacy regulation. While we address specific concerns in the response to comments later in the preamble, in this section, we explore some of the general interaction issues. These summaries do not identify all possible conflicts or overlaps of the privacy regulation and other federal laws, but should provide general guidance for complying with both the privacy regulation and other federal laws. The summaries also provide examples of how covered entities can analyze other federal laws when specific questions arise. HHS may consult with other agencies concerning the interpretation of other federal laws as necessary.

Implied Repeal Analysis

When faced with the need to determine how different federal laws interact with one another, we turn to the judiciary's approach. Courts apply the implied repeal analysis to resolve tensions that appear to exist between two or more statutes. While the implication of a regulation-on-regulation conflict is unclear, courts agree that administrative rules and regulations that do not conflict with express statutory provisions have the force and effect of law. Thus, we believe courts would apply the standard rules of interpretation that apply to statutes to address questions of interpretation with regard to regulatory conflicts.

When faced with two potentially conflicting statutes, courts attempt to construe them so that both are given effect. If this construction is not possible, courts will look for express language in the later statute, or an intent in its legislative history, indicating that Congress intended the later statute to repeal the earlier one. If there is no expressed intent to repeal the earlier statute, courts will characterize the statutes as either general or specific. Ordinarily, later, general statutes will not repeal the special provisions of an earlier, specific statute. In some cases, when a later, general statute creates an irreconcilable conflict or is manifestly inconsistent with the earlier, specific statute in a manner that indicates a clear and manifest Congressional intent to repeal the earlier statute, courts will find that the later statute repeals the earlier statute by implication. In these cases, the latest legislative action may prevail and repeal the prior law, but only to the extent of the conflict.

There should be few instances in which conflicts exist between a statute or regulation and the rules below. For example, if a statute permits a covered entity to disclose protected health information and the rules below permit such a disclosure, no conflict arises; the covered entity could comply with both and choose whether or not to disclose the information. In instances in which a potential conflict appears, we would attempt to resolve it so that both laws applied. For example, if a statute or regulation permits dissemination of protected health information, but the rules below prohibit the use or disclosure without an authorization, we believe a covered entity would be able to comply with both because it could obtain an authorization under § 164.508 before disseminating the information under the other law.

Many apparent conflicts will not be true conflicts. For example, if a conflict

appears to exist because a previous statute or regulation requires a specific use or disclosure of protected health information that the rules below appear to prohibit, the use or disclosure pursuant to that statute or regulation would not be a violation of the privacy regulation because § 164.512(a) permits covered entities to use or disclose protected health information as required by law.

If a statute or regulation prohibits dissemination of protected health information, but the privacy regulation requires that an individual have access to that information, the earlier, more specific statute would apply. The interaction between the Clinical Laboratory Improvement Amendments regulation is an example of this type of conflict. From our review of several federal laws, it appears that Congress did not intend for the privacy regulation to overrule existing statutory requirements in these instances.

Examples of Interaction

We have summarized how certain federal laws interact with the privacy regulation to provide specific guidance in areas deserving special attention and to serve as examples of the analysis involved. In the Response to Comment section, we have provided our responses to specific questions raised during the comment period.

The Privacy Act

The Privacy Act of 1974, 5 U.S.C. 552a, prohibits disclosures of records contained in a system of records maintained by a federal agency (or its contractors) without the written request or consent of the individual to whom the record pertains. This general rule is subject to various statutory exceptions. In addition to the disclosures explicitly permitted in the statute, the Privacy Act permits agencies to disclose information for other purposes compatible with the purpose for which the information was collected by identifying the disclosure as a ''routine use'' and publishing notice of it in the **Federal Register**. The Act applies to all federal agencies and certain federal contractors who operate Privacy Act systems of records on behalf of federal agencies.

Some federal agencies and contractors of federal agencies that are covered entities under the privacy rules are subject to the Privacy Act. These entities must comply with all applicable federal statutes and regulations. For example, if the privacy regulation permits a disclosure, but the disclosure is not permitted under the Privacy Act, the federal agency may not make the disclosure. If, however, the Privacy Act allows a federal agency the discretion to make a routine use disclosure, but the privacy regulation prohibits the disclosure, the federal agency will have to apply its discretion in a way that complies with the regulation. This means not making the particular disclosure.

The Freedom of Information Act

FOIA, 5 U.S.C. 552, provides for public disclosure, upon the request of any person, of many types of information in the possession of the federal government, subject to nine exemptions and three exclusions. For example, Exemption 6 permits federal agencies to withhold ''personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.'' 5 U.S.C. 552(b)(6).

Uses and disclosures required by FOIA come within § 164.512(a) of the privacy regulation that permits uses or disclosures required by law if the uses or disclosures meet the relevant requirements of the law. Thus, a federal agency must determine whether it may apply an exemption or exclusion to redact the protected health information when responding to a FOIA request. When a FOIA request asks for documents that include protected health information, we believe the agency, when appropriate, must apply Exemption 6 to preclude the release of medical files or otherwise redact identifying details before disclosing the remaining information.

We offer the following analysis for federal agencies and federal contractors who operate Privacy Act systems of records on behalf of federal agencies and must comply with FOIA and the privacy regulation. If presented with a FOIA request that would result in the disclosure of protected health information, a federal agency must first determine if FOIA requires the disclosure or if an exemption or exclusion would be appropriate. We believe that generally a disclosure of protected health information, when requested under FOIA, would come within FOIA Exemption 6. We recognize, however, that the application of this exemption to information about deceased individuals requires a different analysis than that applicable to living individuals because, as a general rule, under the Privacy Act, privacy rights are extinguished at death. However, under FOIA, it is entirely appropriate to consider the privacy interests of a decedent's survivors under Exemption 6. See Department of Justice FOIA Guide 2000, Exemption 6: Privacy Considerations. Covered entities subject to FOIA must evaluate each disclosure on a case-by-case basis, as they do now under current FOIA procedures.

Federal Substance Abuse Confidentiality Requirements

The federal confidentiality of substance abuse patient records statute, section 543 of the Public Health Service Act, 42 U.S.C. 290dd-2, and its implementing regulation, 42 CFR part 2, establish confidentiality requirements for patient records that are maintained in connection with the performance of any federally-assisted specialized alcohol or drug abuse program. Substance abuse programs are generally programs or personnel that provide alcohol or drug abuse treatment, diagnosis, or referral for treatment. The term ''federally-assisted'' is broadly defined and includes federally conducted or funded programs, federally licensed or certified programs, and programs that are tax exempt. Certain exceptions apply to information held by the Veterans Administration and the Armed Forces.

There are a number of health care providers that are subject to both these rules and the substance abuse statute and regulations. In most cases, a conflict will not exist between these rules. These privacy rules permit a health care provider to disclose information in a number of situations that are not permitted under the substance abuse regulation. For example, disclosures allowed, without patient authorization, under the privacy rule for law enforcement, judicial and administrative proceedings, public health, health oversight, directory assistance, and as required by other laws would generally be prohibited under the substance abuse statute and regulation. However, because these disclosures are permissive and not mandatory, there is no conflict. An entity would not be in violation of the privacy rules for failing to make these disclosures.

Similarly, provisions in the substance abuse regulation provide for permissive disclosures in case of medical emergencies, to the FDA, for research activities, for audit and evaluation activities, and in response to certain court orders. Because these are permissive disclosures, programs subject to both the privacy rules and the substance abuse rule are able to comply with both rules even if the privacy rules restrict these types of disclosures. In addition, the privacy rules generally require that an individual be given access to his or her own health information. Under the substance abuse

regulation, programs may provide such access, so there is no conflict.

The substance abuse regulation requires notice to patients of the substance abuse confidentiality requirements and provides for written consent for disclosure. While the privacy rules have requirements that are somewhat different, the program may use notice and authorization forms that include all the elements required by both regulations. The substance abuse rule provides a sample notice and a sample authorization form and states that the use of these forms would be sufficient. While these forms do not satisfy all of the requirements of the privacy regulation, there is no conflict because the substance abuse regulation does not mandate the use of these forms.

Employee Retirement Income Security Act of 1974

ERISA was enacted in 1974 to regulate pension and welfare employee benefit plans established by private sector employers, unions, or both, to provide benefits to their workers and dependents. Under ERISA, plans that provide ''through the purchase of insurance or otherwise * * * medical, surgical, or hospital care or benefits, or benefits in the event of sickness, accident, disability, [or] death'' are defined as employee welfare benefit plans. 29 U.S.C. 1002(1). In 1996, HIPAA amended ERISA to require portability, nondiscrimination, and renewability of health benefits provided by group health plans and group health insurance issuers. Numerous, although not all, ERISA plans are covered under the rules proposed below as ''health plans.''

Section 514(a) of ERISA, 29 U.S.C. 1144(a), preempts all state laws that ''relate to'' any employee benefit plan. However, section 514(b) of ERISA, 29 U.S.C. 1144(b)(2)(A), expressly saves from preemption state laws that regulate insurance. Section 514(b)(2)(B) of ERISA, 29 U.S.C. 1144(b)(2)(B), provides that an ERISA plan is deemed not to be an insurer for the purpose of regulating the plan under the state insurance laws. Thus, under the deemer clause, states may not treat ERISA plans as insurers subject to direct regulation by state law. Finally, section 514(d) of ERISA, 29 U.S.C. 1144(d), provides that ERISA does not ''alter, amend, modify, invalidate, impair, or supersede any law of the United States.''

We considered whether the preemption provision of section 264(c)(2) of HIPAA would give effect to state laws that would otherwise be preempted by section 514(a) of ERISA. As discussed above, our reading of the statutes together is that the effect of section 264(c)(2) is only to leave in place state privacy protections that would otherwise apply and that are more stringent than the federal privacy protections.

Many health plans covered by the privacy regulation are also subject to ERISA requirements. Our discussions and consultations have not uncovered any particular ERISA requirements that would conflict with the rules.

The Family Educational Rights and Privacy Act

FERPA, as amended, 20 U.S.C. 1232g, provides parents of students and eligible students (students who are 18 or older) with privacy protections and rights for the records of students maintained by federally funded educational agencies or institutions or persons acting for these agencies or institutions. We have excluded education records covered by FERPA, including those education records designated as education records under Parts B, C, and D of the Individuals with Disabilities Education Act Amendments of 1997, from the definition of protected health information. For example, individually identifiable health information of students under the age of 18 created by a nurse in a primary or secondary school that receives federal funds and that is subject to FERPA is an education record, but not protected health information. Therefore, the privacy regulation does not apply. We followed this course because Congress specifically addressed how information in education records should be protected in FERPA.

We have also excluded certain records, those described at 20 U.S.C. 1232g(a)(4)(B)(iv), from the definition of protected health information because FERPA also provided a specific structure for the maintenance of these records. These are records (1) of students who are 18 years or older or are attending post-secondary educational institutions, (2) maintained by a physician, psychiatrist, psychologist, or recognized professional or paraprofessional acting or assisting in that capacity, (3) that are made, maintained, or used only in connection with the provision of treatment to the student, and (4) that are not available to anyone, except a physician or appropriate professional reviewing the record as designated by the student. Because FERPA excludes these records from its protections only to the extent they are not available to anyone other than persons providing treatment to students, any use or disclosure of the record for other purposes, including providing access to the individual student who is the subject of the information, would turn the record into an education record. As education records, they would be subject to the protections of FERPA.

These exclusions are not applicable to all schools, however. If a school does not receive federal funds, it is not an educational agency or institution as defined by FERPA. Therefore, its records that contain individually identifiable health information are not education records. These records may be protected health information. The educational institution or agency that employs a school nurse is subject to our regulation as a health care provider if the school nurse or the school engages in a HIPAA transaction.

While we strongly believe every individual should have the same level of privacy protection for his/her individually identifiable health information, Congress did not provide us with authority to disturb the scheme it had devised for records maintained by educational institutions and agencies under FERPA. We do not believe Congress intended to amend or preempt FERPA when it enacted HIPAA.

With regard to the records described at 20 U.S.C. 1232g(a)(4)(b)(iv), we considered requiring health care providers engaged in HIPAA transactions to comply with the privacy regulation up to the point these records were used or disclosed for purposes other than treatment. At that point, the records would be converted from protected health information into education records. This conversion would occur any time a student sought to exercise his/her access rights. The provider, then, would need to treat the record in accordance with FERPA's requirements and be relieved from its obligations under the privacy regulation. We chose not to adopt this approach because it would be unduly burdensome to require providers to comply with two different, yet similar, sets of regulations and inconsistent with the policy in FERPA that these records be exempt from regulation to the extent the records were used only to treat the student.

Gramm-Leach-Bliley

In 1999, Congress passed Gramm-Leach-Bliley (GLB), Pub. L. 106–102, which included provisions, section 501 *et seq.*, that limit the ability of financial institutions to disclose ''nonpublic personal information'' about consumers to non-affiliated third parties and require financial institutions to provide customers with their privacy policies and practices with respect to nonpublic

personal information. In addition, Congress required seven agencies with jurisdiction over financial institutions to promulgate regulations as necessary to implement these provisions. GLB and its accompanying regulations define ''financial institutions'' as including institutions engaged in the financial activities of bank holding companies, which may include the business of insuring. See 15 U.S.C. 6809(3); 12 U.S.C. 1843(k). However, Congress did not provide the designated federal agencies with the authority to regulate health insurers. Instead, it provided states with an incentive to adopt and have their state insurance authorities enforce these rules. See 15 U.S.C. 6805. If a state were to adopt laws consistent with GLB, health insurers would have to determine how to comply with both sets of rules.

Thus, GLB has caused concern and confusion among health plans that are subject to our privacy regulation. Although Congress remained silent as to its understanding of the interaction of GLB and HIPAA's privacy provisions, the Federal Trade Commission and other agencies implementing the GLB privacy provisions noted in the preamble to their GLB regulations that they ''would consult with HHS to avoid the imposition of duplicative or inconsistent requirements.'' 65 Fed. Reg. 33646, 33648 (2000). Additionally, the FTC also noted that ''persons engaged in providing insurance'' would be within the enforcement jurisdiction of state insurance authorities and not within the jurisdiction of the FTC. *Id.*

Because the FTC has clearly stated that it will not enforce the GLB privacy provisions against persons engaged in providing insurance, health plans will not be subject to dual federal agency jurisdiction for information that is both nonpublic personal information and protected health information. If states choose to adopt GLB-like laws or regulations, which may or may not track the federal rules completely, health plans would need to evaluate these laws under the preemption analysis described in subpart B of Part 160.

Federally Funded Health Programs

These rules will affect various federal programs, some of which may have requirements that are, or appear to be, inconsistent with the requirements of these regulations. These programs include those operated directly by the federal government (such as health programs for military personnel and veterans) as well as programs in which health services or benefits are provided by the private sector or by state or local governments, but which are governed by various federal laws (such as Medicare, Medicaid, and ERISA).

Congress explicitly included some of these programs in HIPAA, subjecting them directly to the privacy regulation. Section 1171 of the Act defines the term ''health plan'' to include the following federally conducted, regulated, or funded programs: Group plans under ERISA that either have 50 or more participants or are administered by an entity other than the employer who established and maintains the plan; federally qualified health maintenance organizations; Medicare; Medicaid; Medicare supplemental policies; the health care program for active military personnel; the health care program for veterans; the Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); the Indian health service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, *et seq.*; and the Federal Employees Health Benefits Program. There also are many other federally conducted, regulated, or funded programs in which individually identifiable health information is created or maintained, but which do not come within the statutory definition of ''health plan.'' While these latter types of federally conducted, regulated, or assisted programs are not explicitly covered by part C of title XI in the same way that the programs listed in the statutory definition of ''health plan'' are covered, the statute may nonetheless apply to transactions and other activities conducted under such programs. This is likely to be the case when the federal entity or federally regulated or funded entity provides health services; the requirements of part C may apply to such an entity as a ''health care provider.'' Thus, the issue of how different federal requirements apply is likely to arise in numerous contexts.

There are a number of authorities under the Public Health Service Act and other legislation that contain explicit confidentiality requirements, either in the enabling legislation or in the implementing regulations. Many of these are so general that there would appear to be no problem of inconsistency, in that nothing in those laws or regulations would appear to restrict the provider's ability to comply with the privacy regulation's requirements.

There may, however, be authorities under which either the requirements of the enabling legislation or of the program regulations would impose requirements that differ from these rules.

For example, regulations applicable to the substance abuse block grant program funded under section 1943(b) of the Public Health Service Act require compliance with 42 CFR part 2, and, thus, raise the issues identified above in the substance abuse confidentiality regulations discussion. There are a number of federal programs which, either by statute or by regulation, restrict the disclosure of patient information to, with minor exceptions, disclosures ''required by law.'' See, for example, the program of projects for prevention and control of sexually transmitted diseases funded under section 318(e)(5) of the Public Health Service Act (42 CFR 51b.404); the regulations implementing the community health center program funded under section 330 of the Public Health Service Act (42 CFR 51c.110); the regulations implementing the program of grants for family planning services under title X of the Public Health Service Act (42 CFR 59.15); the regulations implementing the program of grants for black lung clinics funded under 30 U.S.C. 437(a) (42 CFR 55a.104); the regulations implementing the program of maternal and child health projects funded under section 501 of the Act (42 CFR 51a.6); the regulations implementing the program of medical examinations of coal miners (42 CFR 37.80(a)). These legal requirements would restrict the grantees or other entities providing services under the programs involved from making many of the disclosures that §§ 164.510 or 164.512 would permit. In some cases, permissive disclosures for treatment, payment, or health care operations would also be limited. Because §§ 164.510 and 164.512 are merely permissive, there would not be a conflict between the program requirements, because it would be possible to comply with both. However, entities subject to both sets of requirements would not have the total range of discretion that they would have if they were subject only to this regulation.

Food, Drug, and Cosmetic Act

The Food, Drug, and Cosmetic Act, 21 U.S.C. 301, *et seq.*, and its accompanying regulations outline the responsibilities of the Food and Drug Administration with regard to monitoring the safety and effectiveness of drugs and devices. Part of the agency's responsibility is to obtain reports about adverse events, track medical devices, and engage in other types of post marketing surveillance. Because many of these reports contain protected health information, the information within them may come within the purview of the privacy rules.

Although some of these reports are required by the Food, Drug, and Cosmetic Act or its accompanying regulations, other types of reporting are voluntary. We believe that these reports, while not mandated, play a critical role in ensuring that individuals receive safe and effective drugs and devices. Therefore, in § 164.512(b)(1)(iii), we have provided that covered entities may disclose protected health information to a person subject to the jurisdiction of the Food and Drug Administration for specified purposes, such as reporting adverse events, tracking medical devices, or engaging in other post marketing surveillance. We describe the scope and conditions of such disclosures in more detail in § 164.512(b).

Clinical Laboratory Improvement Amendments

CLIA, 42 U.S.C. 263a, and the accompanying regulations, 42 CFR part 493, require clinical laboratories to comply with standards regarding the testing of human specimens. This law requires clinical laboratories to disclose test results or reports only to authorized persons, as defined by state law. If a state does not define the term, the federal law defines it as the person who orders the test.

We realize that the person ordering the test is most likely a health care provider and not the individual who is the subject of the protected health information included within the result or report. Under this requirement, therefore, a clinical laboratory may be prohibited by law from providing the individual who is the subject of the test result or report with access to this information.

Although we believe individuals should be able to have access to their individually identifiable health information, we recognize that in the specific area of clinical laboratory testing and reporting, the Health Care Financing Administration, through regulation, has provided that access may be more limited. To accommodate this requirement, we have provided at § 164.524(1)(iii) that covered entities maintaining protected health information that is subject to the CLIA requirements do not have to provide individuals with a right of access to or a right to inspect and obtain a copy of this information if the disclosure of the information to the individual would be prohibited by CLIA.

Not all clinical laboratories, however, will be exempted from providing individuals with these rights. If a clinical laboratory operates in a state in which the term ''authorized person'' is defined to include the individual, the clinical laboratory would have to provide the individual with these rights. Similarly, if the individual was the person who ordered the test and an authorized person included such a person, the laboratory would be required to provide the individual with these rights.

Additionally, CLIA regulations exempt the components or functions of ''research laboratories that test human specimens but do not report patient specific results for the diagnosis, prevention or treatment of any disease or impairment of, or the assessment of the health of individual patients'' from the CLIA regulatory scheme. 42 CFR 493.3(a)(2). If subject to the access requirements of this regulation, such entities would be forced to meet the requirements of CLIA from which they are currently exempt. To eliminate this additional regulatory burden, we have also excluded covered entities that are exempt from CLIA under that rule from the access requirement of this regulation.

Although we are concerned about the lack of immediate access by the individual, we believe that, in most cases, individuals who receive clinical tests will be able to receive their test results or reports through the health care provider who ordered the test for them. The provider will receive the information from the clinical laboratory. Assuming that the provider is a covered entity, the individual will have the right of access and right to inspect and copy this protected health information through his or her provider.

Other Mandatory Federal or State Laws

Many federal laws require covered entities to provide specific information to specific entities in specific circumstances. If a federal law requires a covered entity to disclose a specific type of information, the covered entity would not need an authorization under § 164.508 to make the disclosure because the final rule permits covered entities to make disclosures that are required by law under § 164.512(a). Other laws, such as the Social Security Act (including its Medicare and Medicaid provisions), the Family and Medical Leave Act, the Public Health Service Act, Department of Transportation regulations, the Environmental Protection Act and its accompanying regulations, the National Labor Relations Act, the Federal Aviation Administration, and the Federal Highway Administration rules, may also contain provisions that require covered entities or others to use or disclose protected health information for specific purposes.

When a covered entity is faced with a question as to whether the privacy regulation would prohibit the disclosure of protected health information that it seeks to disclose pursuant to a federal law, the covered entity should determine if the disclosure is required by that law. In other words, it must determine if the disclosure is mandatory rather than merely permissible. If it is mandatory, a covered entity may disclose the protected health information pursuant to § 164.512(a), which permits covered entities to disclose protected health information without an authorization when the disclosure is required by law. If the disclosure is not required (but only permitted) by the federal law, the covered entity must determine if the disclosure comes within one of the other permissible disclosures. If the disclosure does not come within one of the provisions for permissible disclosures, the covered entity must obtain an authorization from the individual who is the subject of the information or de-identify the information before disclosing it.

If another federal law prohibits a covered entity from using or disclosing information that is also protected health information, but the privacy regulation permits the use or disclosure, a covered entity will need to comply with the other federal law and not use or disclose the information.

Federal Disability Nondiscrimination Laws

The federal laws barring discrimination on the basis of disability protect the confidentiality of certain medical information. The information protected by these laws falls within the larger definition of ''health information'' under this privacy regulation. The two primary disability nondiscrimination laws are the Americans with Disabilities Act (ADA), 42 U.S.C. 12101 *et seq.*, and the Rehabilitation Act of 1973, as amended, 29 U.S.C. 701 *et seq.*, although other laws barring discrimination on the basis of disability (such as the nondiscrimination provisions of the Workforce Investment Act of 1988, 29 U.S.C. 2938) may also apply. Federal disability nondiscrimination laws cover two general categories of entities relevant to this discussion: employers and entities that receive federal financial assistance.

Employers are not covered entities under the privacy regulation. Many employers, however, are subject to the federal disability nondiscrimination laws and, therefore, must protect the

confidentiality of all medical information concerning their applicants and employees.

The employment provisions of the ADA, 42 U.S.C. 12111 *et seq.*, expressly cover employers of 15 or more employees, employment agencies, labor organizations, and joint labor-management committees. Since 1992, employment discrimination complaints arising under sections 501, 503, and 504 of the Rehabilitation Act also have been subject to the ADA's employment nondiscrimination standards. See ''Rehabilitation Act Amendments,'' Pub. L. No. 102–569, 106 Stat. 4344. Employers subject to ADA nondiscrimination standards have confidentiality obligations regarding applicant and employee medical information. Employers must treat such medical information, including medical information from voluntary health or wellness programs and any medical information that is voluntarily disclosed as a confidential medical record, subject to limited exceptions.

Transmission of health information by an employer to a covered entity, such as a group health plan, is governed by the ADA confidentiality restrictions. The ADA, however, has been interpreted to permit an employer to use medical information for insurance purposes. See 29 CFR part 1630 App. at § 1630.14(b) (describing such use with reference to 29 CFR 1630.16(f), which in turn explains that the ADA regulation ''is not intended to disrupt the current regulatory structure for self-insured employers * * * or current industry practices in sales, underwriting, pricing, administrative and other services, claims and similar insurance related activities based on classification of risks as regulated by the states''). See also, ''Enforcement Guidance on Disability-Related Inquiries and Medical Examinations of Employees under the Americans with Disabilities Act,'' 4, n.10 (July 26, 2000), FEP Manual (BNA) (''Enforcement Guidance on Employees''). See generally, ''ADA Enforcement Guidance on Preemployment Disability-Related Questions and Medical Examinations'' (October 10, 1995), 8 FEP Manual (BNA) 405:7191 (1995) (also available at *http://www.eeoc.gov*). Thus, use of medical information for insurance purposes may include transmission of health information to a covered entity.

If an employer-sponsored group health plan is closely linked to an employer, the group health plan may be subject to ADA confidentiality restrictions, as well as this privacy regulation. *See Carparts Distribution Center, Inc.* v. *Automotive Wholesaler's Association of New England, Inc.,* 37 F.3d 12 (1st Cir. 1994)(setting forth three bases for ADA Title I jurisdiction over an employer-provided medical reimbursement plan, in a discrimination challenge to the plan's HIV/AIDS cap). Transmission of applicant or employee health information by the employer's management to the group health plan may be permitted under the ADA standards as the use of medical information for insurance purposes. Similarly, disclosure of such medical information by the group health plan, under the limited circumstances permitted by this privacy regulation, may involve use of the information for insurance purposes as broadly described in the ADA discussion above.

Entities that receive federal financial assistance, which may also be covered entities under the privacy regulation, are subject to section 504 of the Rehabilitation Act (29 U.S.C. 794) and its implementing regulations. Each federal agency has promulgated such regulations that apply to entities that receive financial assistance from that agency (''recipients''). These regulations may limit the disclosure of medical information about persons who apply to or participate in a federal financially assisted program or activity. For example, the Department of Labor's section 504 regulation (found at 29 CFR part 32), consistent with the ADA standards, requires recipients that conduct employment-related programs, including employment training programs, to maintain confidentiality regarding any information about the medical condition or history of applicants to or participants in the program or activity. Such information must be kept separate from other information about the applicant or participant and may be provided to certain specified individuals and entities, but only under certain limited circumstances described in the regulation. See 29 CFR 32.15(d). Apart from those circumstances, the information must be afforded the same confidential treatment as medical records, *id.* Also, recipients of federal financial assistance from the Department of Health and Human Services, such as hospitals, are subject to the ADA's employment nondiscrimination standards. They must, accordingly, maintain confidentiality regarding the medical condition or history of applicants for employment and employees.

The statutes and implementing regulations under which the federal financial assistance is provided may contain additional provisions regulating collection and disclosure of medical, health, and disability-related information. See, *e.g.,* section 188 of the Workforce Investment Act of 1988 (29 U.S.C. 2938) and 29 CFR 37.3(b). Thus, covered entities that are subject to this privacy regulation, may also be subject to the restrictions in these laws as well.

U.S. Safe Harbor Privacy Principles (European Union Directive on Data Protection)

The E.U. Directive became effective in October 1998 and prohibits European Union Countries from permitting the transfer of personal data to another country without ensuring that an ''adequate level of protection,'' as determined by the European Commission, exists in the other country or pursuant to one of the Directive's derogations of this rule, such as pursuant to unambiguous consent or to fulfill a contract with the individual. In July 2000, the European Commission concluded that the U.S. Safe Harbor Privacy Principles [1] constituted ''adequate protection.'' Adherence to the Principles is voluntary. Organizations wishing to engage in the exchange of personal data with E.U. countries may assert compliance with the Principles as one means of obtaining data from E.U. countries.

The Department of Commerce, which negotiated these Principles with the European Commission, has provided guidance for U.S. organizations seeking to adhere to the guidelines and comply with U.S. law. We believe this guidance addresses the concerns covered entities seeking to transfer personal data from E.U. countries may have. When ''U.S. law imposes a conflicting obligation, U.S. organizations whether in the safe harbor or not must comply with the law.'' An organization does not need to comply with the Principles if a conflicting U.S. law ''explicitly authorizes'' the particular conduct. The organization's non-compliance is ''limited to the extent necessary to meet the overriding legitimate interests further[ed] by such authorization.'' However, if only a difference exists such that an ''option is allowable under the Principles and/or U.S. law, organizations are expected to opt for the higher protection where possible.'' Questions regarding compliance and interpretation will be decided based on U.S. law. See Department of Commerce, Memorandum on Damages for Breaches

[1] The Principles are: (1) Notice; (2) Choice (*i.e.,* consent); (3) Onward Transfer (i.e., subsequent disclosures); (4) Security; (5) Data Integrity; (6) Access; and (7) Enforcement. Department of Commerce, Safe Harbor Principles, July 21, 2000 (''Principles''). They do not apply to manually processed data.

of Privacy, Legal Authorizations and Mergers and Takeovers in U.S. Law 5 (July 17, 2000); Department of Commerce, Safe Harbor Privacy Principles Issued by the U.S. Department of Commerce on July 21, 2000, 65 FR 45666 (2000). The Principles and our privacy regulation are based on common principles of fair information practices. We believe they are essentially consistent and that an organization complying with our privacy regulation can fairly and correctly self-certify that it complies with the Principles. If a true conflict arises between the privacy regulation and the Principles, the Department of Commerce's guidance provides that an entity must comply with the U.S. law.

Part 160—Subpart C—Compliance and Enforcement

Proposed § 164.522 included five paragraphs addressing activities related to the Secretary's enforcement of the rule. These provisions were based on procedures and requirements in various civil rights regulations. Proposed § 164.522(a) provided that the Secretary would, to the extent practicable, seek the cooperation of covered entities in obtaining compliance, and could provide technical assistance to covered entities to help them comply voluntarily. Proposed § 164.522(b) provided that individuals could file complaints with the Secretary. However, where the complaint related to the alleged failure of a covered entity to amend or correct protected health information as proposed in the rule, the Secretary would not make certain determinations such as whether protected health information was accurate or complete. This paragraph also listed the requirements for filing complaints and indicated that the Secretary may investigate such complaints and what might be reviewed as part of such investigation.

Under proposed § 164.522(c), the Secretary would be able to conduct compliance reviews. Proposed § 164.522(d) described the responsibilities that covered entities keep records and reports as prescribed by the Secretary, cooperate with compliance reviews, permit the Secretary to have access to their facilities, books, records, and other sources of information during normal business hours, and seek records held by other persons. This paragraph also stated that the Secretary would maintain the confidentiality of protected health information she collected and prohibit covered entities from taking retaliatory action against individuals for filing complaints or for other activities. Proposed § 164.522(e) provided that the Secretary would inform the covered entity and the individual complainant if an investigation or review indicated a failure to comply and would seek to resolve the matter informally if possible. If the matter could not be resolved informally, the Secretary would be able to issue written findings, be required to inform the covered entity and the complainant, and be able to pursue civil enforcement action or make a criminal referral. The Secretary would also be required to inform the covered entity and the individual complainant if no violation was found.

We make the following changes and additions to proposed § 164.522 in the final rule. First, we have moved this section to part 160, as a new subpart C, ''Compliance and Enforcement.'' Second, we add new sections that explain the applicability of these provisions and incorporate certain definitions. Accordingly, we change the proposed references to violations to ''this subpart'' to violations of ''the applicable requirements of part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.'' Third, the final rule at § 160.306(a) provides that any person, not just an ''individual'' (the person who is the subject of the individually identifiable health information) may file a complaint with the Secretary. Other references in this subpart to an individual have been changed accordingly. Fourth, we delete the proposed § 164.522(a) language that indicated that the Secretary would not determine whether information was accurate or complete, or whether errors or omissions might have an adverse effect on the individual. While the policy is not changed in that the Secretary will not make such determinations, we believe the language is unnecessary and may suggest that we would make all other types of determinations, such as all determinations in which the regulation defers to the professional judgment of the covered entity. Fifth, § 160.306(b)(3) requires that complaints be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred, unless this time limit is waived by the Secretary for good cause shown. Sixth, § 160.310(b) requires cooperation with investigations as well as compliance reviews. Seventh, § 160.310 (c)(1) provides that the Secretary must be provided access to a covered entity's facilities, books, records, accounts, and other sources of information, including protected health information, at any time and without notice where exigent circumstances exist, such as where documents might be hidden or destroyed. Eighth, the provision proposed at § 164.522(d) that would prohibit covered entities from taking retaliatory action against individuals for filing a complaint with the Secretary or for certain other actions has been changed and moved to § 164.530. Ninth, § 160. 312(a)(2) deletes the reference in the proposed rule to using violation findings as a basis for initiating action to secure penalties. This deletion is not a substantive change. This language was removed because penalties will be addressed in the enforcement regulation. As in the NPRM, the Secretary may promulgate alternative procedures for complaints relating to national security. For example, to protect classified information, we may promulgate rules that would allow an intelligence community agency to create a separate body within that agency to receive complaints.

The Department plans to issue an Enforcement Rule that applies to all of the regulations that the Department issues under the Administrative Simplification provisions of HIPAA. This regulation will address the imposition of civil monetary penalties and the referral of criminal cases where there has been a violation of this rule. Penalties are provided for under section 262 of HIPAA. The Enforcement Rule would also address the topics covered by Subpart C below. It is expected that this Enforcement Rule would replace Subpart C.

Part 164—Subpart A—General Provisions

Section 164.102—Statutory Basis

In the NPRM, we provided that the provisions of this part are adopted pursuant to the Secretary's authority to prescribe standards, requirements, and implementation standards under part C of title XI of the Act and section 264 of Public Law 104–191. The final rule adopts this language.

Section 164.104—Applicability

In the NPRM, we provided that except as otherwise provided, the provisions of this part apply to covered entities: health plans, health care clearinghouses, and health care providers who transmit health information in electronic form in connection with any transaction referred to in section 1173(a)(1) of the Act. The final rule adopts this language.

Section 164.106—Relationship to Other Parts

The final rule adds a new provision stating that in complying with the requirements of this part, covered entities are required to comply with the applicable provisions of parts 160 and 162 of this subchapter. This language references Subchapter C in this regulation, Administrative Data Standards and Related Requirements; Part 160, General Administrative Requirements; and Part 162, Administrative Requirements. Part 160 includes requirements such as keeping records and submitting compliance reports to the Secretary and cooperating with the Secretary's complaint investigations and compliance reviews. Part 162 includes requirements such as requiring a covered entity that conducts an electronic transaction, adopted under this part, with another covered entity to conduct the transaction as a standard transaction as adopted by the Secretary.

Part 164—Subpart B–D—Reserved

Part 164—Subpart E—Privacy

Section 164.500—Applicability

The discussion below describes the entities and the information that are subject to the final regulation.

Many of the provisions of the regulation are presented as ''standards.'' Generally, the standards indicate what must be accomplished under the regulation and implementation specifications describe how the standards must be achieved.

Covered Entities

We proposed in the NPRM to apply the standards in the regulation to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with transactions referred to in section 1173(a)(1) of the Act. The proposal referred to these entities as ''covered entities.''

We have revised § 164.500 to clarify the applicability of the rule to health care clearinghouses. As we stated in the preamble to the NPRM, we believe that in most instances health care clearinghouses will receive protected health information as a business associate to another covered entity. This understanding was confirmed by the comments and by our fact finding. Clearinghouses rarely have direct contact with individuals, and usually will not be in a position to create protected health information or to receive it directly from them. Unlike health plans and providers, clearinghouses usually convey and repackage information and do not add materially to the substance of protected health information of an individual.

The revised language provides that clearinghouses are not subject to certain requirements in the rule when acting as business associates of other covered entities. As revised, a clearinghouse acting as a business associate is subject only to the provisions of this section, to the definitions, to the general rules for uses and disclosures of protected health information (subject to limitations), to the provision relating to health care components, to the provisions relating to uses and disclosures for which consent, individual authorization or an opportunity to agree or object is not required (subject to limitations), to the transition requirements and to the compliance date. With respect to the uses and disclosures authorized under § 164.502 or § 164.512, a clearinghouse acting as a business associate is not authorized by the rule to make any use or disclosure not permitted by its business associate contract. Clearinghouses acting as business associates are not subject to the other requirements of this rule, which include the provisions relating to procedural requirements, requirements for obtaining consent, individual authorization or agreement, provision of a notice, individual rights to request privacy protection, access and amend information and receive an accounting of disclosures and the administrative requirements.

We note that, even as business associates, clearinghouses remain covered entities. Clearinghouses, like other covered entities, are responsible under this regulation for abiding by the terms of business associate contracts. For example, while the provisions regarding individuals' access to and right to request corrections to protected health information about them apply only to health plans and covered health care providers, clearinghouses may have some responsibility for providing such access under their business associate contracts. A clearinghouse (or any other covered entity) that violates the terms of a business associate contract also is in direct violation of this rule and, as a covered entity, is subject to compliance and enforcement action.

We clarify that a covered entity is only subject to these rules to the extent that they possess protected health information. Moreover, these rules only apply with regard to protected health information. For example, if a covered entity does not disclose or receive from its business associate any protected health information and no protected health information is created or received by its business associate on behalf of the covered entity, then the business associate requirements of this rule do not apply.

We clarify that the Department of Defense or any other federal agency and any non-governmental organization acting on its behalf, is not subject to this rule when it provides health care in another country to foreign national beneficiaries. The Secretary believes that this exemption is warranted because application of the rule could have the unintended effect of impeding or frustrating the conduct of such activities, such as interfering with the ability of military command authorities to obtain protected health information on prisoners of war, refugees, or detainees for whom they are responsible under international law. See the preamble to the definition of ''individual'' for further discussion.

Covered Information

We proposed in the NPRM to apply the requirements of the rule to individually identifiable health information that is or has been electronically transmitted or maintained by a covered entity. The provisions would have applied to the information itself, referred to as protected health information in the rule, and not to the particular records in which the information is contained. We proposed that once information was maintained or transmitted electronically by a covered entity, the protections would follow the information in whatever form, including paper records, in which it exists while held by a covered entity. The proposal would not have applied to information that was never electronically maintained or transmitted by a covered entity.

In the final rule, we extend the scope of protections to all individually identifiable health information in any form, electronic or non-electronic, that is held or transmitted by a covered entity. This includes individually identifiable health information in paper records that never has been electronically stored or transmitted. (See § 164.501, definition of ''protected health information,'' for further discussion.)

Section 164.501—Definitions

Correctional Institution

The proposed rule did not define the term correctional institution. The final rule defines correctional institution as any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States,

a state, a territory, a political subdivision of a state or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. Other persons held in lawful custody includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial. This language was necessary to explain the privacy rights and protections of inmates in this regulation.

Covered Functions

We add a new term, ''covered functions,'' as a shorthand way of expressing and referring to the functions that the entities covered by section 1172(a) of the Act perform. Section 1171 defines the terms ''health plan'', ''health care provider'', and ''health care clearinghouse'' in functional terms. Thus, a ''health plan'' is an individual or group plan ''that provides, or pays the cost of, medical care * * *'', a ''health care provider'' ''furnish[es] health care services or supplies,'' and a ''health care clearinghouse'' is an entity ''that processes or facilitates the processing of * * * data elements of health information * * *''. Covered functions, therefore, are the activities that any such entity engages in that are directly related to operating as a health plan, health care provider, or health care clearinghouse; that is, they are the functions that make it a health plan, health care provider, or health care clearinghouse.

The term ''covered functions'' is not intended to include various support functions, such as computer support, payroll and other office support, and similar support functions, although we recognize that these support functions must occur in order for the entity to carry out its health care functions. Because such support functions are often also performed for parts of an organization that are not doing functions directly related to the health care functions and may involve access to and/or use of protected health information, the rules below describe requirements for ensuring that workforce members who perform these support functions do not impermissibly use or disclose protected health information. See § 164.504.

Data Aggregation

The NPRM did not include a definition of data aggregation. In the final rule, data aggregation is defined, with respect to protected health information received by a business associate in its capacity as the business associate of a covered entity, as the combining of such protected health information by the business associate with protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit the creation of data for analyses that relate to the health care operations of the respective covered entities. The definition is included in the final rule to help describe how business associates can assist covered entities to perform health care operations that involve comparative analysis of protected health information from otherwise unaffiliated covered entities. Data aggregation is a service that gives rise to a business associate relationship if the performance of the service involves disclosure of protected health information by the covered entity to the business associate.

Designated Record Set

In the proposed rule, we defined designated record set as ''a group of records under the control of a covered entity from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual and which is used by the covered entity to make decisions about the individual.'' We defined a ''record'' as ''any item, collection, or grouping of protected health information maintained, collected, used, or disseminated by a covered entity.''

In the final rule, we modify the definition of designated record set to specify certain records maintained by or for a covered entity that are always part of a covered entity's designated record sets and to include other records that are used to make decisions about individuals. We do not use the means of retrieval of a record as a defining criteria.

For health plans, designated record sets include, at a minimum, the enrollment, payment, claims adjudication, and case or medical management record systems of the plan. For covered health care providers, designated record sets include, at a minimum, the medical record and billing record about individuals maintained by or for the provider. In addition to these records, designated record sets include any other group of records that are used, in whole or in part, by or for a covered entity to make decisions about individuals. We note that records that otherwise meet the definition of designated record set and which are held by a business associate of the covered entity are part of the covered entity's designated record sets. Although we do not specify particular types of records that are always included in the designated record sets of clearinghouses when they are not acting as business associates, this definition includes a group of records that such a clearinghouse uses, in whole or in part, to make decisions about individuals.

For the most part we retain, with slight modifications, the definition of ''record,'' defining it as any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated.

Direct Treatment Relationship

This term was not included in the proposed rule. Direct treatment relationship means a relationship between a health care provider and an individual that is not an indirect treatment relationship (see definition of indirect treatment relationship, below). For example, outpatient pharmacists and Web-based providers generally have direct treatment relationships with patients. Outpatient pharmacists fill prescriptions written by other providers, but they furnish the prescription and advice about the prescription directly to the patient, not through another treating provider. Web-based providers generally deliver health care independently, without the orders of another provider.

A provider may have direct treatment relationships with some patients and indirect treatment relationships with others. In some provisions of the final rule, providers with indirect treatment relationships are excepted from requirements that apply to other providers. See § 164.506 regarding consent for uses and disclosures of protected health information for treatment, payment, and health care operations, and § 164.520 regarding notice of information practices. These exceptions apply only with respect to the individuals with whom the provider has an indirect treatment relationship.

Disclosure

We proposed to define ''disclosure'' to mean the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information. The final rule is unchanged. We note that the transfer of protected health information from a covered entity to a business associate is a disclosure for purposes of this regulation.

Health Care Operations

The preamble to the proposed rule explained that in order for treatment and payment to occur, protected health

information must be used within entities and shared with business partners. In the proposed rule we provided a definition for ''health care operations'' to clarify the activities we considered to be ''compatible with and directly related to'' treatment and payment and for which protected health information could be used or disclosed without individual authorization. These activities included conducting quality assessment and improvement activities, reviewing the competence or qualifications and accrediting/licensing of health care professionals and plans, evaluating health care professional and health plan performance, training future health care professionals, insurance activities relating to the renewal of a contract for insurance, conducting or arranging for medical review and auditing services, and compiling and analyzing information in anticipation of or for use in a civil or criminal legal proceeding. Recognizing the dynamic nature of the health care industry, we acknowledged that the specified categories may need to be modified as the industry evolves.

The preamble discussion of the proposed general rules listed certain activities that would not be considered health care operations because they were sufficiently unrelated to treatment and payment to warrant requiring an individual to authorize such use or disclosure. Those activities included: marketing of health and non-health items and services; disclosure of protected health information for sale, rent or barter; use of protected health information by a non-health related division of an entity; disclosure of protected health information for eligibility, enrollment, underwriting, or risk rating determinations prior to an individuals' enrollment in a health plan; disclosure to an employer for employment determinations; and fundraising.

In the final rule, we do not change the general approach of defining health care operations: health care operations are the listed activities undertaken by the covered entity that maintains the protected health information (*i.e.,* one covered entity may not disclose protected health information for the operations of a second covered entity); a covered entity may use any protected health information it maintains for its operations (*e.g.,* a plan may use protected health information about former enrollees as well as current enrollees); we expand the proposed list to reflect many changes requested by commenters.

We modify the proposal that health care operations represent activities ''in support of'' treatment and payment functions. Instead, in the final rule, health care operations are the enumerated activities to the extent that the activities are related to the covered entity's functions as a health care provider, health plan or health care clearinghouse, *i.e.,* the entity's ''covered functions.'' We make this change to clarify that health care operations includes general administrative and business functions necessary for the covered entity to remain a viable business. While it is possible to draw a connection between all the enumerated activities and ''treatment and payment,'' for some general business activities (*e.g.,* audits for financial disclosure statements) that connection may be tenuous. The proposed concept also did not include the operations of those health care clearinghouses that may be covered by this rule outside their status as business associate to a covered entity. We expand the definition to include disclosures for the enumerated activities of organized health care arrangements in which the covered entity participates. See also the definition of organized health care arrangements, below.

In addition, we make the following changes and additions to the enumerated subparagraphs:

(1) We add language to clarify that the primary purpose of the studies encompassed by ''quality assessment and improvement activities'' must not be to obtain generalizable knowledge. A study with such a purpose would meet the rule's definition of research, and use or disclosure of protected health information would have to meet the requirements of §§ 164.508 or 164.512(i). Thus, studies may be conducted as a health care operation if development of generalizable knowledge is not the primary goal. However, if the study changes and the covered entity intends the results to be generalizable, the change should be documented by the covered entity as proof that, when initiated, the primary purpose was health care operations.

We add population-based activities related to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives, and related functions that do not entail direct patient care. Many commenters recommended adding the term ''disease management'' to health care operations. We were unable, however, to find a generally accepted definition of the term. Rather than rely on this label, we include many of the functions often included in discussions of disease management in this definition or in the definition of treatment. This topic is discussed further in the comment responses below.

(2) We have deleted ''undergraduate and graduate'' as a qualifier for ''students,'' to make the term more general and inclusive. We add the term ''practitioners.'' We expand the purposes encompassed to include situations in which health care providers are working to improve their skills. The rule also adds the training of non-health care professionals.

(3) The rule expands the range of insurance related activities to include those related to the creation, renewal or replacement of a contract for health insurance or health benefits, as well as ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss and excess of loss insurance). For these activities, we also eliminate the proposed requirement that these uses and disclosures apply only to protected health information about individuals already enrolled in a health plan. Under this provision, a group health plan that wants to replace its insurance carrier may disclose certain protected health information to insurance issuers in order to obtain bids on new coverage, and an insurance carrier interested in bidding on new business may use protected health information obtained from the potential new client to develop the product and pricing it will offer. For circumstances in which no new contract is issued, we add a provision in § 164.514(g) restricting the recipient health plan from using or disclosing protected health information obtained for this purpose, other than as required by law. Uses and disclosures in these cases come within the definition of ''health care operations,'' provided that the requirements of § 164.514(g) are met, if applicable. See § 164.504(f) for requirements for such disclosures by group health plans, as well as specific restrictions on the information that may be disclosed to plan sponsors for such purposes. We note that a covered health care provider must obtain an authorization under § 164.508 in order to disclose protected health information about an individual for purposes of pre-enrollment underwriting; the underwriting is not an ''operation'' of the provider and that disclosure is not otherwise permitted by a provision of this rule.

(4) We delete reference to the ''compiling and analyzing information in anticipation of or for use in a civil or criminal legal proceeding'' and replace it with a broader reference to

conducting or arranging for ''legal services.''

We add two new categories of activities:

(5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies.

(6) Business management activities and general administrative functions, such as management activities relating to implementation of and compliance with the requirements of this subchapter, fundraising for the benefit of the covered entity to the extent permitted without authorization under § 164.514(f), and marketing of certain services to individuals served by the covered entity, to the extent permitted without authorization under § 164.514(e) (see discussion in the preamble to that section, below). For example, under this category we permit uses or disclosures of protected health information to determine from whom an authorization should be obtained, for example to generate a mailing list of individuals who would receive an authorization request.

We add to the definition of health care operations disclosure of protected health information for due diligence to a covered entity that is a potential successor in interest. This provision includes disclosures pursuant to the sale of a covered entity's business as a going concern, mergers, acquisitions, consolidations, and other similar types of corporate restructuring between covered entities, including a division of a covered entity, and to an entity that is not a covered entity but will become a covered entity if the transfer or sale is completed. Other types of sales of assets, or disclosures to organizations that are not and would not become covered entities, are not included in the definition of health care operations and could only occur if the covered entity obtained valid authorization for such disclosure in accordance with § 164.508, or if the disclosure is otherwise permitted under this rule.

We also add to health care operations disclosure of protected health information for resolution of internal grievances. These uses and disclosures include disclosure to an employee and/or employee representative, for example when the employee needs protected health information to demonstrate that the employer's allegations of improper conduct are untrue. We note that such employees and employee representatives are not providing services to or for the covered entity, and, therefore, no business associate contract is required. Also included are resolution of disputes from patients or enrollees regarding the quality of care and similar matters.

We also add use for customer service, including the provision of data and statistical analyses for policyholders, plan sponsors, or other customers, as long as the protected health information is not disclosed to such persons. We recognize that part of the general management of a covered entity is customer service. We clarify that customer service may include the use of protected health information to provide data and statistical analyses. For example, a plan sponsor may want to understand why its costs are rising faster than average, or why utilization in one plant location is different than in another location. An association that sponsors an insurance plan for its members may want information on the relative costs of its plan in different areas. Some plan sponsors may want more detailed analyses that attempt to identify health problems in a work site. We note that when a plan sponsor has several different group health plans, or when such plans provide insurance or coverage through more than one health insurance issuer or HMO, the covered entities may jointly engage in this type of analysis as a health care operation of the organized health care arrangement.

This activity qualifies as a health care operation only if it does not result in the disclosure of protected health information to the customer. The results of the analyses must be presented in a way that does not disclose protected health information. A disclosure of protected health information to the customer as a health care operation under this provision violates this rule. This provision is not intended to permit covered entities to circumvent other provisions in this rule, including requirements relating to disclosures of protected health information to plan sponsors or the requirements relating to research. See § 164.504(f) and § 164.512(i).

We use the term customer to provide flexibility to covered entities. We do not intend the term to apply to persons with whom the covered entity has no other business; this provision is intended to permit covered entities to provide service to their existing customer base.

We note that this definition, either alone or in conjunction with the definition of ''organized health care arrangement,'' allows an entity such as an integrated staff model HMO, whether legally integrated or whether a group of associated entities, that hold themselves out as an organized arrangement to share protected health information under § 164.506. In these cases, the sharing of protected health information will be either for the operations of the disclosing entity or for the organized health care arrangement in which the entity is participating.

Whether a disclosure is allowable for health care operations under this provision is determined separately from whether a business associate contract is required. These provisions of the rule operate independently. Disclosures for health care operations may be made to an entity that is neither a covered entity nor a business associate of the covered entity. For example, a covered academic medical center may disclose certain protected health information to community health care providers who participate in one of its continuing medical education programs, whether or not such providers are covered health care providers under this rule. A provider attending a continuing education program is not thereby performing services for the covered entity sponsoring the program and, thus, is not a business associate for that purpose. Similarly, health plans may disclose for due diligence purposes to another entity that may or may not be a covered entity or a business associate.

Health Oversight Agency

The proposed rule would have defined ''health oversight agency'' as ''an agency, person, or entity, including the employees or agents thereof, (1) That is: (i) A public agency; or (ii) A person or entity acting under grant of authority from or contract with a public agency; and (2) Which performs or oversees the performance of any audit; investigation; inspection; licensure or discipline; civil, criminal, or administrative proceeding or action; or other activity necessary for appropriate oversight of the health care system, of government benefit programs for which health information is relevant to beneficiary eligibility, or of government regulatory programs for which health information is necessary for determining compliance with program standards.'' The proposed rule also described the functions of health oversight agencies in the proposed health oversight section (§ 164.510(c)) by repeating much of this definition.

In the final rule, we modify the definition of health oversight agency by eliminating from the definition the language in proposed § 164.510(c) (now § 164.512(d)). In addition, the final rule clarifies this definition by specifying that a ''health oversight agency'' is an agency or authority of the United States,

a state, a territory, a political subdivision of a state or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or grantees, that is authorized by law to oversee the health care system or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

The preamble to the proposed rule listed the following as examples of health oversight agencies that conduct oversight activities relating to the health care system: state insurance commissions, state health professional licensure agencies, Offices of Inspectors General of federal agencies, the Department of Justice, state Medicaid fraud control units, Defense Criminal Investigative Services, the Pension and Welfare Benefit Administration, the HHS Office for Civil Rights, and the FDA. The proposed rule listed the Social Security Administration and the Department of Education as examples of health oversight agencies that conduct oversight of government benefit programs for which health information is relevant to beneficiary eligibility. The proposed rule listed the Occupational Health and Safety Administration and the Environmental Protection Agency as examples of oversight agencies that conduct oversight of government regulatory programs for which health information is necessary for determining compliance with program standards.

In the final rule, we include the following as additional examples of health oversight activities: (1) The U.S. Department of Justice's civil rights enforcement activities, and in particular, enforcement of the Civil Rights of Institutionalized Persons Act (42 U.S.C. 1997–1997j) and the Americans with Disabilities Act (42 U.S.C. 12101 *et seq.*), as well as the EEOC's civil rights enforcement activities under titles I and V of the ADA; (2) the FDA's oversight of food, drugs, biologics, devices, and other products pursuant to the Food, Drug, and Cosmetic Act (21 U.S.C. 301 *et seq.*) and the Public Health Service Act (42 U.S.C. 201 *et seq.*); and (3) data analysis —performed by a public agency or by a person or entity acting under grant of authority from or under contract with a public agency —to detect health care fraud.

''Overseeing the health care system,'' which is included in the definition of health oversight, encompasses activities such as: oversight of health care plans; oversight of health benefit plans; oversight of health care providers; oversight of health care and health care delivery; oversight activities that involve resolution of consumer complaints; oversight of pharmaceuticals, medical products and devices, and dietary supplements; and a health oversight agency's analysis of trends in health care costs, quality, health care delivery, access to care, and health insurance coverage for health oversight purposes.

We recognize that health oversight agencies, such as the U.S. Department of Labor's Pension and Welfare Benefits Administration, may perform more than one type of health oversight. For example, agencies may sometimes perform audits and investigations and at other times conduct general oversight of health benefit plans. Such entities are considered health oversight agencies under the rule for any and all of the health oversight functions that they perform.

The definition of health oversight agency does not include private organizations, such as private-sector accrediting groups. Accreditation organizations are performing health care operations functions on behalf of health plans and covered health care providers. Accordingly, in order to obtain protected health information without individuals' authorizations, accrediting groups must enter into business associate agreements with health plans and covered health care providers for these purposes. Similarly, private entities, such as coding committees, that help government agencies that are health plans make coding and payment decisions are performing health care payment functions on behalf the government agencies and, therefore, must enter into business associate agreements in order to receive protected health information from the covered entity (absent individuals' authorization for such disclosure).

Indirect Treatment Relationship

This term was not included in the proposed rule. An ''indirect treatment relationship'' is a relationship between a health care provider and an individual in which the provider delivers health care to the individual based on the orders of another health care provider and the health care services, products, diagnoses, or results are typically furnished to the patient through another provider, rather than directly. For example, radiologists and pathologists generally have indirect treatment relationships with patients because they deliver diagnostic services based on the orders of other providers and the results of those services are furnished to the patient through the direct treating provider. This definition is necessary to clarify the relationships between providers and individuals in the regulation. For example, see the consent discussion at § 164.506.

Individual

We proposed to define ''individual'' to mean the person who is the subject of the protected health information. We proposed that the term include, with respect to the signing of authorizations and other rights (such as access, copying, and correction), the following types of legal representatives:

(1) With respect to adults and emancipated minors, legal representatives (such as court-appointed guardians or persons with a power of attorney), to the extent to which applicable law permits such legal representatives to exercise the person's rights in such contexts.

(2) With respect to unemancipated minors, a parent, guardian, or person acting in loco parentis, provided that when a minor lawfully obtains a health care service without the consent of or notification to a parent, guardian, or other person acting in *loco parentis,* the minor shall have the exclusive right to exercise the rights of an individual with respect to the protected health information relating to such care.

(3) With respect to deceased persons, an executor, administrator, or other person authorized under applicable law to act on behalf of the decedent's estate.

In addition, we proposed to exclude from the definition:

(1) Foreign military and diplomatic personnel and their dependents who receive health care provided by or paid for by the Department of Defense or other federal agency or by an entity acting on its behalf, pursuant to a country-to-country agreement or federal statute.

(2) Overseas foreign national beneficiaries of health care provided by the Department of Defense or other federal agency or by a non-governmental organization acting on its behalf.

In the final rule, we eliminate from the definition of ''individual'' the provisions designating a legal representative as the ''individual'' for purposes of exercising certain rights with regard to protected health information. Instead, we include in the final rule a separate standard for ''personal representatives.'' A covered entity must treat a personal representative of an individual as the individual except under specified circumstances. See discussion in

§ 164.502(g) regarding personal representatives.

In addition, we eliminate from the definition of ''individual'' the above exclusions for foreign military and diplomatic personnel and overseas foreign national beneficiaries. We address the special circumstances for use and disclosure of protected health information about individuals who are foreign military personnel in § 164.512(k). We address overseas foreign national beneficiaries in § 164.500, ''Applicability.'' The protected health information of individuals who are foreign diplomatic personnel and their dependents are not subject to special treatment under the final rule.

Individually identifiable health information about one individual may exist in the health records of another individual; health information about one individual may include health information about a second person. For example, a patient's medical record may contain information about the medical conditions of the patient's parents, children, and spouse, as well as their names and contact information. For the purpose of this rule, if information about a second person is included within the protected health information of an individual, the second person is not the person who is the subject of the protected health information. The second person is not the ''individual'' with regard to that protected health information, and under this rule thus does not have the individual's rights (*e.g.,* access and amendment) with regard to that information.

Individually Identifiable Health Information

We proposed to define ''individually identifiable health information'' to mean information that is a subset of health information, including demographic information collected from an individual, and that:

(1) Is created by or received from a health care provider, health plan, employer, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and

(i) Which identifies the individual, or

(ii) With respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

In the final rule, we change ''created by or received from a health care provider * * *'' to ''created or received by a health care provider * * * ''in order to conform to the statute. We otherwise retain the definition of ''individually identifiable health information'' without change in the final rule.

Inmate

The proposed rule did not define the term inmate. In the final rule, it is defined as a person incarcerated in or otherwise confined to a correctional institution. The addition of this definition is necessary to explain the privacy rights and protections of inmates in this regulation.

Law Enforcement Official

The proposed rule would have defined a ''law enforcement official'' as ''an official of an agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, who is empowered by law to conduct: (1) An investigation or official proceeding inquiring into a violation of, or failure to comply with, any law; or (2) a criminal, civil, or administrative proceeding arising from a violation of, or failure to comply with, any law.''

The final rule modifies this definition slightly. The definition in the final rule recognizes that law enforcement officials are empowered to prosecute cases as well as to conduct investigations and civil, criminal, or administrative proceedings. In addition, the definition in the final rule reflects the fact that when investigations begin, often it is not clear that law has been violated. Thus, the final rule describes law enforcement investigations and official proceedings as inquiring into a potential violation of law. In addition, it describes law enforcement-related civil, criminal, or administrative proceedings as arising from alleged violation of law.

Marketing

The proposed rule did not include a definition of ''marketing.'' The proposed rule generally required that a covered entity would need an authorization from an individual to use or disclose protected health information for marketing.

In the final rule we define marketing as a communication about a product or service a purpose of which is to encourage recipients of the communication to purchase or use the product or service. The definition does not limit the type or means of communication that are considered marketing.

The definition of marketing contains three exceptions. If a covered entity receives direct or indirect remuneration from a third party for making a written communication otherwise described in an exception, then the communication is not excluded from the definition of marketing. The activities we except from the definition of marketing are encompassed by the definitions of treatment, payment, and health care operations. Covered entities may therefore use and disclose protected health information for these excepted activities without authorization under § 164.508 and pursuant to any applicable consent obtained under § 164.506.

The first exception applies to communications made by a covered entity for the purpose of describing the entities participating in a provider network or health plan network. It also applies to communications made by a covered entity for the purpose of describing if and the extent to which a product or service, or payment for a product or service, is provided by the covered entity or included in a benefit plan. This exception permits covered entities to use or disclose protected health information when discussing topics such as the benefits and services available under a health plan, the payment that may be made for a product or service, which providers offer a particular product or service, and whether a provider is part of a network or whether (and what amount of) payment will be provided with respect to the services of particular providers. This exception expresses our intent not to interfere with communications made to individuals about their health benefits.

The second exception applies to communications tailored to the circumstances of a particular individual, made by a health care provider to an individual as part of the treatment of the individual, and for the purpose of furthering the treatment of that individual. This exception leaves health care providers free to use or disclose protected health information as part of a discussion of its products and services, or the products and services of others, and to prescribe, recommend, or sell such products or services, as part of the treatment of an individual. This exception includes activities such as referrals, prescriptions, recommendations, and other communications that address how a product or service may relate to the individual's health. This exception expresses our intent not to interfere with communications made to individuals about their treatment.

The third exception applies to communications tailored to the

circumstances of a particular individual and made by a health care provider or health plan to an individual in the course of managing the treatment of that individual or for the purpose of directing or recommending to that individual alternative treatments, therapies, providers, or settings of care. As with the previous exception, this exception permits covered entities to discuss freely their products and services and the products and services of third parties, in the course of managing an individual's care or providing or discussing treatment alternatives with an individual, even when such activities involve the use or disclose protected health information.

Section 164.514 contains provisions governing use or disclosure of protected health information in marketing communications, including a description of certain marketing communications that may use or include protected health information but that may be made by a covered entity without individual authorization. The definition of health care operations includes those marketing communications that may be made without an authorization pursuant to § 164.514. Covered entities may therefore use and disclose protected health information for these activities pursuant to any applicable consent obtained under § 164.506, or, if they are not required to obtain a consent under § 164.506, without one.

Organized Health Care Arrangement

This term was not used in the proposed rule. We define the term in order to describe certain arrangements in which participants need to share protected health information about their patients to manage and benefit the common enterprise. To allow uses and disclosures of protected health information for these arrangements, we also add language to the definition of ''health care operations.'' See discussion of that term above.

We include five arrangements within the definition of organized health care arrangement. The arrangements involve clinical or operational integration among legally separate covered entities in which it is often necessary to share protected health information for the joint management and operations of the arrangement. They may range in legal structure, but a key component of these arrangements is that individuals who obtain services from them have an expectation that these arrangements are integrated and that they jointly manage their operations. We include within the definition a clinically integrated care setting in which individuals typically receive health care from more than one health care provider. Perhaps the most common example of this type of organized health care arrangement is the hospital setting, where a hospital and a physician with staff privileges at the hospital together provide treatment to the individual. Participants in such clinically integrated settings need to be able to share health information freely not only for treatment purposes, but also to improve their joint operations. For example, any physician with staff privileges at a hospital must be able to participate in the hospital's morbidity and mortality reviews, even when the particular physician's patients are not being discussed. Nurses and other hospital personnel must also be able to participate. These activities benefit the common enterprise, even when the benefits to a particular participant are not evident. While protected health information may be freely shared among providers for treatment purposes under other provisions of this rule, some of these joint activities also support the health care operations of one or more participants in the joint arrangement. Thus, special rules are needed to ensure that this rule does not interfere with legitimate information sharing among the participants in these arrangements.

We also include within the definition an organized system of health care in which more than one covered entity participates, and in which the participating covered entities hold themselves out to the public as participating in a joint arrangement, and in which the joint activities of the participating covered entities include at least one of the following: utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf; quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or payment activities, if the financial risk for delivering health care is shared in whole or in part by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk. A common example of this type of organized health care arrangement is an independent practice association formed by a large number of physicians. They may advertise themselves as a common enterprise (*e.g.,* Acme IPA), whether or not they are under common ownership or control, whether or not they practice together in an integrated clinical setting, and whether or not they share financial risk.

If such a group engages jointly in one or more of the listed activities, the participating covered entities will need to share protected health information to undertake such activities and to improve their joint operations. In this example, the physician participants in the IPA may share financial risk through common withhold pools with health plans or similar arrangements. The IPA participants who manage the financial arrangements need protected health information about all the participants' patients in order to manage the arrangement. (The participants may also hire a third party to manage their financial arrangements.) If the participants in the IPA engage in joint quality assurance or utilization review activities, they will need to share protected health information about their patients much as participants in an integrated clinical setting would. Many joint activities that require the sharing of protected health information benefit the common enterprise, even when the benefits to a particular participant are not evident.

We include three relationships related to group health plans as organized health care arrangements. First, we include a group health plan and an issuer or HMO with respect to the group health plan within the definition, but only with respect to the protected health information of the issuer or HMO that relates to individuals who are or have been participants or beneficiaries in the group health plan. We recognize that many group health plans are funded partially or fully through insurance, and that in some cases the group health plan and issuer or HMO need to coordinate operations to properly serve the enrollees. Second, we include a group health plan and one or more other group health plans each of which are maintained by the same plan sponsor. We recognize that in some instances plan sponsors provide health benefits through a combination of group health plans, and that they may need to coordinate the operations of such plans to better serve the participants and beneficiaries of the plans. Third, we include a combination of group health plans maintained by the same plan sponsor and the health insurance issuers and HMOs with respect to such plans, but again only with respect to the protected health information of such issuers and HMOs that relates to

individuals who are or have been enrolled in such group health plans. We recognize that is some instances a plan sponsor may provide benefits through more than one group health plan, and that such plans may fund the benefits through one or more issuers or HMOs. Again, coordinating health care operations among these entities may be necessary to serve the participants and beneficiaries in the group health plans. We note that the necessary coordination may necessarily involve the business associates of the covered entities and may involve the participation of the plan sponsor to the extent that it is providing plan administration functions and subject to the limits in § 164.504.

Payment

We proposed the term payment to mean:

(1) The activities undertaken by or on behalf of a covered entity that is:

(i) A health plan, or by a business partner on behalf of a health plan, to obtain premiums or to determine or fulfill its responsibility for coverage under the health plan and for provision of benefits under the health plan; or

(ii) A health care provider or health plan, or a business partner on behalf of such provider or plan, to obtain reimbursement for the provision of health care.

(2) Activities that constitute payment include:

(i) Determinations of coverage, adjudication or subrogation of health benefit claims;

(ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics;

(iii) Billing, claims management, and medical data processing;

(iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; and

(v) Utilization review activities, including precertification and preauthorization of services.

In the final rule, we maintain the general approach of defining of payment: payment activities are described generally in the first clause of the definition, and specific examples are given in the second clause. Payment activities relate to the covered entity that maintains the protected health information (*i.e.,* one covered entity may not disclose protected health information for the payment activities of a second covered entity). A covered entity may use or disclose only the protected health information about the individual to whom care was rendered, for its payment activities (*e.g.,* a provider may disclose protected health information only about the patient to whom care was rendered in order to obtain payment for that care, or only the protected health information about persons enrolled in the particular health plan that seeks to audit the provider's records). We expand the proposed list to reflect many changes requested by commenters.

We add eligibility determinations as an activity included in the definition of payment. We expand coverage determinations to include the coordination of benefits and the determination of a specific individual's cost sharing amounts. The rule deletes activities related to the improvement of methods of paying or coverage policies from this definition and instead includes them in the definition of health care operations. We add to the definition ''collection activities.'' We replace ''medical data processing'' activities with health care data processing related to billing, claims management, and collection activities. We add activities for the purpose of obtaining payment under a contract for reinsurance (including stop-loss and excess of loss insurance). Utilization review activities now include concurrent and retrospective review of services.

In addition, we modify this definition to clarify that the activities described in section 1179 of the Act are included in the definition of ''payment.'' We add new subclause (vi) allowing covered entities to disclose to consumer reporting agencies an individual's name, address, date of birth, social security number and payment history, account number, as well as the name and address of the individual's health care provider and/or health plan, as appropriate. Covered entities may make disclosure of this protected health information to consumer reporting agencies for purposes related to collection of premiums or reimbursement. This allows reporting not just of missed payments and overdue debt but also of subsequent positive payment experience (*e.g.,* to expunge the debt). We consider such positive payment experience to be ''related to'' collection of premiums or reimbursement.

The remaining activities described in section 1179 are included in other language in this definition. For example, ''authorizing, processing, clearing, settling, billing, transferring, reconciling or collecting, a payment for, or related to, health plan premiums or health care'' are covered by paragraph (2)(iii) of the definition, which allows use and disclosure of protected health information for ''billing, claims management, collection activities and related health care data processing.'' ''Claims management'' also includes auditing payments, investigating and resolving payment disputes and responding to customer inquiries regarding payments. Disclosure of protected health information for compliance with civil or criminal subpoenas, or with other applicable laws, are covered under § 164.512 of this regulation. (See discussion above regarding the interaction between 1179 and this regulation.)

We modify the proposed regulation text to clarify that payment includes activities undertaken to reimburse health care providers for treatment provided to individuals.

Covered entities may disclose protected health information for payment purposes to any other entity, regardless of whether it is a covered entity. For example, a health care provider may disclose protected health information to a financial institution in order to cash a check or to a health care clearinghouse to initiate electronic transactions. However, if a covered entity engages another entity, such as a billing service or a financial institution, to conduct payment activities on its behalf, the other entity may meet the definition of ''business associate'' under this rule. For example, an entity is acting as a business associate when it is operating the accounts receivable system on behalf of a health care provider.

Similarly, payment includes disclosure of protected health information by a health care provider to an insurer that is not a ''health plan'' as defined in this rule, to obtain payment. For example, protected health information may be disclosed to obtain reimbursement from a disability insurance carrier. We do not interpret the definition of ''payment'' to include activities that involve the disclosure of protected health information by a covered entity, including a covered health care provider, to a plan sponsor for the purpose of obtaining payment under a group health plan maintained by such plan sponsor, or for the purpose of obtaining payment from a health insurance issuer or HMO with respect to a group health plan maintained by such plan sponsor, unless the plan sponsor is performing plan administration pursuant to § 164.504(f).

The Transactions Rule adopts standards for electronic health care transactions, including two for processing payments. We adopted the ASC X12N 835 transaction standard for ''Health Care Payment and Remittance

Advice'' transactions between health plans and health care providers, and the ASC X12N 820 standard for ''Health Plan Premium Payments'' transactions between entities that arrange for the provision of health care or provide health care coverage payments and health plans. Under these two transactions, information to effect funds transfer is transmitted in a part of the transaction separable from the part containing any individually identifiable health information.

We note that a covered entity may conduct the electronic funds transfer portion of the two payment standard transactions with a financial institution without restriction, because it contains no protected health information. The protected health information contained in the electronic remittance advice or the premium payment enrollee data portions of the transactions is not necessary either to conduct the funds transfer or to forward the transactions. Therefore, a covered entity may not disclose the protected health information to a financial institution for these purposes. A covered entity may transmit the portions of the transactions containing protected health information through a financial institution if the protected health information is encrypted so it can be read only by the intended recipient. In such cases no protected health information is disclosed and the financial institution is acting solely as a conduit for the individually identifiable data.

Plan Sponsor

In the final rule we add a definition of ''plan sponsor.'' We define plan sponsor by referencing the definition of the term provided in (3)(16)(B) of the Employee Retirement Income Security Act (ERISA). The plan sponsor is the employer or employee organization, or both, that establishes and maintains an employee benefit plan. In the case of a plan established by two or more employers, it is the association, committee, joint board of trustees, or other similar group or representative of the parties that establish and maintain the employee benefit plan. This term includes church health plans and government health plans. Group health plans may disclose protected health information to plan sponsors who conduct payment and health care operations activities on behalf of the group health plan if the requirements for group health plans in § 164.504 are met.

The preamble to the Transactions Rule noted that plan sponsors of group health plans are not covered entities and, therefore, are not required to use the standards established in that regulation to perform electronic transactions, including enrollment and disenrollment transactions. We do not change that policy through this rule. Plan sponsors that perform enrollment functions are doing so on behalf of the participants and beneficiaries of the group health plan and not on behalf of the group health plan itself. For purposes of this rule, plan sponsors are not subject to the requirements of § 164.504 regarding group health plans when conducting enrollment activities.

Protected Health Information

We proposed to define ''protected health information'' to mean individually identifiable health information that is or has been electronically maintained or electronically transmitted by a covered entity, as well as such information when it takes any other form. For purposes of this definition, we proposed to define ''electronically transmitted'' as including information exchanged with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, transmissions over the Internet, Extranet, leased lines, dial-up lines, private networks, telephone voice response, and ''faxback'' systems. We proposed that this definition not include ''paper-to-paper'' faxes, or person-to-person telephone calls, video teleconferencing, or messages left on voice-mail.

Further, ''electronically maintained'' was proposed to mean information stored by a computer or on any electronic medium from which the information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, or compact disc optical media.

The proposal's definition explicitly excluded:

(1) Individually identifiable health information that is part of an ''education record'' governed by the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g.

(2) Individually identifiable health information of inmates of correctional facilities and detainees in detention facilities.

In this final rule we expand the definition of protected health information to encompass all individually identifiable health information transmitted or maintained by a covered entity, regardless of form. Specifically, we delete the conditions for individually identifiable health information to be ''electronically maintained'' or ''electronically transmitted'' and the corresponding definitions of those terms. Instead, the final rule defines protected health information to be individually identifiable health information that is:

(1) Transmitted by electronic media;

(2) Maintained in any medium described in the definition of electronic media at § 162.103 of this subchapter; or

(3) Transmitted or maintained in any other form or medium.

We refer to electronic media, as defined in § 162.103, which means the mode of electronic transmission. It includes the Internet (wide-open), Extranet (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, private networks, and those transmissions that are physically moved from one location to another using magnetic tape, disk, or compact disk media.

The definition of protected health information is set out in this form to emphasize the severability of this provision. As discussed below, we believe we have ample legal authority to cover all individually identifiable health information transmitted or maintained by covered entities. We have structured the definition this way so that, if a court were to disagree with our view of our authority in this area, the rule would still be operational, albeit with respect to a more limited universe of information.

Other provisions of the rules below may also be severable, depending on their scope and operation. For example, if the rule itself provides a fallback, as it does with respect to the various discretionary uses and disclosures permitted under § 164.512, the provisions would be severable under case law.

The definition in the final rule retains the exception relating to individually identifiable health information in ''education records'' governed by FERPA. We also exclude the records described in 20 U.S.C. 1232g(a)(4)(B)(iv). These are records of students held by post-secondary educational institutions or of students 18 years of age or older, used exclusively for health care treatment and which have not been disclosed to anyone other than a health care provider at the student's request. (See discussion of FERPA above.)

We have removed the exception for individually identifiable health information of inmates of correctional facilities and detainees in detention facilities. Individually identifiable health information about inmates is protected health information under the final rule, and special rules for use and disclosure of the protected health

information about inmates and their ability to exercise the rights granted in this rule are described below.

Psychotherapy Notes

Section 164.508(a)(3)(iv)(A) of the proposed rule defined psychotherapy notes as notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session. The proposed definition excluded medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis and progress. Furthermore, we stated in the preamble of the proposed rule that psychotherapy notes would have to be maintained separately from the medical record.

In this final rule, we retain the definition of psychotherapy notes that we had proposed, but add to the regulation text the requirement that, to meet the definition of psychotherapy notes, the information must be separated from the rest of the individual's medical record.

Public Health Authority

The proposed rule would have defined ''public health authority'' as ''an agency or authority of the United States, a state, a territory, or an Indian tribe that is responsible for public health matters as part of its official mandate.''

The final rule changes this definition slightly to clarify that a ''public health authority'' also includes a person or entity acting under a grant of authority from or contract with a public health agency. Therefore, the final rule defines this term as an agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

Required By Law

In the preamble to the NPRM, we did not include a definition of ''required by law.'' We discussed what it meant for an action to be considered to be ''required'' or ''mandated'' by law and included several examples of activities that would be considered as required by law for the purposes of the proposed rule, including a valid Inspector General subpoena, grand jury subpoena, civil investigative demand, or a statute or regulation requiring production of information justifying a claim would constitute a disclosure required by law.

In the final rule we include a new definition, move the preamble clarifications to the regulatory text and add several items to the illustrative list. For purposes of this regulation, ''required by law'' means a mandate contained in law that compels a covered entity to make a use or disclosure of protected health information and that is enforceable in a court of law. Among the examples listed in definition are Medicare conditions of participation with respect to health care providers participating in that program, court-ordered warrants, and subpoenas issued by a court. We note that disclosures ''required by law'' include disclosures of protected health information required by this regulation in § 164.502(a)(2). It does not include contracts between private parties or similar voluntary arrangements. This list is illustrative only and is not intended in any way to limit the scope of this paragraph or other paragraphs in § 164.512 that permit uses or disclosures to the extent required by other laws. We note that nothing in this rule compels a covered entity to make a use or disclosure required by the legal demands or prescriptions listed in this clarification or by any other law or legal process, and a covered entity remains free to challenge the validity of such laws and processes.

Research

We proposed to define ''research'' as it is defined in the Federal Policy for the Protection of Human Subjects, at 45 CFR part 46, subpart A (referred to elsewhere in this rule as ''Common Rule''), and in addition, elaborated on the meaning of the term ''generalizable knowledge.'' In § 164.504 of the proposed rule we defined research as ''* * * a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge. 'Generalizable knowledge' is knowledge related to health that can be applied to populations outside of the population served by the covered entity.''

The final rule eliminates the further elaboration of ''generalizable knowledge.'' Therefore, the rule defines ''research'' as the term is defined in the Common Rule: a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge.

Research Information Unrelated to Treatment

We delete this definition and the associated requirements from the final rule. Refer to § 164.508(f) for new requirements regarding authorizations for research that includes treatment of the individual.

Treatment

The proposed rule defined ''treatment'' as the provision of health care by, or the coordination of health care (including health care management of the individual through risk assessment, case management, and disease management) among, health care providers; the referral of a patient from one provider to another; or the coordination of health care or other services among health care providers and third parties authorized by the health plan or the individual. The preamble noted that the definition was intended to relate only to services provided to an individual and not to an entire enrolled population.

In the final rule, we do not change the general approach to defining treatment: treatment means the listed activities undertaken by any health care provider, not just a covered health care provider. A plan can disclose protected health information to any health care provider to assist the provider's treatment activities; and a health care provider may use protected health information about an individual to treat another individual. A health care provider may use any protected health information it maintains for treatment purposes (*e.g.,* a provider may use protected health information about former patients as well as current patients). We modify the proposed list of treatment activities to reflect changes requested by commenters.

Specifically, we modify the proposed definition of ''treatment'' to include the management of health care and related services. Under the definition, the provision, coordination, or management of health care or related services may be undertaken by one or more health care providers. ''Treatment'' includes coordination or management by a health care provider with a third party and consultation between health care providers. The term also includes referral by a health care provider of a patient to another health care provider.

Treatment refers to activities undertaken on behalf of a single patient, not a population. Activities are considered treatment only if delivered

by a health care provider or a health care provider working with another party. Activities of health plans are not considered to be treatment. Many services, such as a refill reminder communication or nursing assistance provided through a telephone service, are considered treatment activities if performed by or on behalf of a health care provider, such as a pharmacist, but are regarded as health care operations if done on behalf of a different type of entity, such as a health plan.

We delete specific reference to risk assessment, case management, and disease management. Activities often referred to as risk assessment, disease and case management are treatment activities only to the extent that they are services provided to a particular patient by a health care provider; population based analyses or records review for the purposes of treatment protocol development or modification are health care operations, not treatment activities. If a covered entity is licensed as both a health plan and a health care provider, a single activity could be considered to be both treatment and health care operations; for compliance purposes we would consider the purpose of the activity. Given the integration of the health care system we believe that further classification of activities into either treatment or health care operations would not be helpful. See the definition of health care operations for additional discussion.

Use

We proposed to define ''use'' to mean the employment, application, utilization, examination, or analysis of information within an entity that holds the information. In the final rule, we clarify that use refers to the use of individually identifiable health information. We replace the term ''holds'' with the term ''maintains.'' These changes are for clarity only, and are not intended to effect any substantive change.

Section 164.502—General Rules for Uses and Disclosures of Protected Health Information

Section 164.502(a)—Use and Disclosure for Treatment, Payment and Health Care Operations

As a general rule, we proposed in the NPRM to prohibit covered entities from using or disclosing protected health information except as authorized by the individual who is the subject of such information or as explicitly permitted by the rule. The proposed rule explicitly would have permitted covered entities to use or disclose an individual's protected health information without authorization for treatment, payment, and health care operations. The proposal would not have restricted to whom disclosures could be made for the purposes of treatment, payment, or operations. The proposal would have allowed disclosure of the protected health information of one individual for the treatment or payment of another, as appropriate. We also proposed to prohibit covered entities from seeking individual authorization for uses and disclosures for treatment, payment, and health care operations unless required by state or other applicable law.

We proposed two exceptions to this general rule which prohibited covered entities from using or disclosing research information unrelated to treatment or psychotherapy notes for treatment, payment, or health care operations purposes unless a specific authorization was obtained from the subject of the information. In addition, we proposed that a covered entity be prohibited from conditioning treatment, enrollment in a health plan or payment decisions on a requirement that the individual provide a specific authorization for the disclosure of these two types of information (see proposed § 164.508(a)(3)(iii)).

We also proposed to permit covered entities to use or disclose an individual's protected health information for specified public and public policy-related purposes, including public health, research, health oversight, law enforcement, and use by coroners. In addition, the proposal would have permitted covered entities to use and disclose protected health information when required to do so by other law or pursuant to an authorization from the individual allowing them to use or disclose the information for purposes other than treatment, payment or health care operations.

We proposed to require covered entities to disclose protected health information for only two purposes: to permit individuals to inspect and copy protected health information about themselves and for enforcement of the rule.

We proposed not to require covered entities to vary the level of protection accorded to protected health information based on the sensitivity of such information. In addition, we proposed to require that each affected entity assess its own needs and devise, implement, and maintain appropriate privacy policies, procedures, and documentation to address its business requirements.

In the final rule, the general standard remains that covered entities may use or disclose protected health information only as permitted or required by this rule. However, we make significant changes to the conditions under which uses and disclosures are permitted.

We revise the application of the general standard to require covered health care providers who have a direct treatment relationship with an individual to obtain a general ''consent'' from the individual in order to use or disclose protected health information about the individual for treatment, payment and health care operations (for details on who must obtain such consents and the requirements they must meet, see § 164.506). These consents are intended to accommodate both the covered provider's need to use or disclose protected health information for treatment, payment, and health care operations, and also the individual's interest in understanding and acquiescing to such uses and disclosures. In general, other covered entities are permitted to use and disclose protected health information to carry out treatment, payment, or health care operations (as defined in this rule) without obtaining such consent, as in the proposed rule. Covered entities must, as under the proposed rule, obtain the individual's ''authorization'' in order to use or disclose psychotherapy notes for most purposes: see § 164.508(a)(2) for exceptions to this rule. We delete the proposed special treatment of ''research information unrelated to treatment.''

We revise the application of the general standard to require all covered entities to obtain the individual's verbal ''agreement'' before using or disclosing protected health information for facility directories, to persons assisting in the individual's care, and for other purposes described in § 164.510. Unlike ''consent'' and ''authorization,'' verbal agreement may be informal and implied from the circumstances (for details on who must obtain such agreements and the requirements they must meet, see § 164.510). Verbal agreements are intended to accommodate situations where it is neither appropriate to remove from the individual the ability to control the protected health information nor appropriate to require formal, written permission to share such information. For the most part, these provisions reflect current practices.

As under the proposed rule, we permit covered entities to use or disclose protected health information without the individual's consent, authorization or agreement for specified

public policy purposes, in compliance with the requirements in § 164.512.

We permit covered entities to disclose protected health information to the individual who is the subject of that information without any condition. We note that this may include disclosures to ''personal representatives'' of individuals as provided by § 164.502(g).

We permit a covered entity to use or disclose protected health information for other lawful purposes if the entity obtains a written ''authorization'' from the individual, consistent with the provisions of § 164.508. Unlike ''consents,'' these ''authorizations'' are specific and detailed. (For details on who must obtain such authorizations and the requirements they must meet, see § 164.508.) They are intended to provide the individuals with concrete information about, and control over, the uses and disclosures of protected health information about themselves.

The final rule retains the provision that requires a covered entity to disclose protected health information only in two instances: When individuals request access to information about themselves, and when disclosures are compelled by the Secretary for compliance and enforcement purposes.

Finally, § 164.502(a)(1) also requires covered entities to use or disclose protected health information in compliance with the other provisions of § 164.502, for example, consistent with the minimum necessary standard, to create de-identified information, or to a personal representative of an individual. These provisions are described below.

We note that a covered entity may use or disclose protected health information as permitted by and in accordance with a provision of this rule, regardless of whether that use or disclosure fails to meet the requirements for use or disclosure under another provision of this rule.

Section 164.502(b)—Minimum Necessary Uses and Disclosures

The proposed rule required a covered entity to make all reasonable efforts not to use or disclose more than the minimum amount of protected health information necessary to accomplish the intended purpose of the use or disclosure (proposed § 164.506(b)). This final rule significantly modifies the proposed requirements for implementing the minimum necessary standard. In the final rule, § 164.502(b) contains the basic standard and § 164.514 describes the requirements for implementing the standard. Therefore we discuss all aspects of the minimum necessary standard and specific requirements below in the discussion of § 164.514(d).

Section 164.502(c)—Uses and Disclosures Under a Restriction Agreement

The proposed rule would have required that covered health care providers permit individuals to request restrictions of uses and disclosures of protected health information and would have prohibited covered providers from using or disclosing protected health information in violation of any agreed-to restriction.

The final rule retains an individual's right to request restrictions on uses or disclosures for treatment, payment or health care operations and prohibits a covered entity from using or disclosing protected health information in a way that is inconsistent with an agreed upon restriction between the covered entity and the individual, but makes some changes to this right. Most significantly, under the final rule individuals have the right to request restrictions of all covered entities. This standard is set forth in § 164.522. Details about the changes to the standard are explained in the preamble discussion to § 164.522.

Section 164.502(d)—Creation of De-identified Information

In proposed § 164.506(d) of the NPRM, we proposed to permit use of protected health information for the purpose of creating de-identified information and we provided detailed mechanisms for doing so.

In § 164.502(d) of the final rule, we permit a covered entity to use protected health information to create de-identified information, whether or not the de-identified information is to be used by the covered entity. We clarify that de-identified information created in accordance with our procedures (which have been moved to § 164.514(a)) is not subject to the requirements of these privacy rules unless it is re-identified. Disclosure of a key or mechanism that could be used to re-identify such information is also defined to be disclosure of protected health information. See the preamble to § 164.514(a) for further discussion.

Section 164.502(e)—Business Associates

In the proposed rule, other than for purposes of consultation or referral for treatment, we would have allowed a covered entity to disclose protected health information to a business partner only pursuant to a written contract that would, among other specified provisions, limit the business partner's uses and disclosures of protected health information to those permitted by the contract, and would impose certain security, inspection and reporting requirements on the business partner. We proposed to define the term ''business partner'' to mean, with respect to a covered entity, a person to whom the covered entity discloses protected health information so that the person can carry out, assist with the performance of, or perform on behalf of, a function or activity for the covered entity.

In the final rule, we change the term ''business partner'' to ''business associate'' and in the definition clarify the full range of circumstances in which a person is acting as a business associate of a covered entity. (See definition of ''business associate'' in § 160.103.) These changes mean that § 164.502(e) requires a business associate contract (or other arrangement, as applicable) not only when the covered entity discloses protected health information to a business associate, but also when the business associate creates or receives protected health information on behalf of the covered entity.

In the final rule, we modify the proposed standard and implementation specifications for business associates in a number of significant ways. These modifications are explained in the preamble discussion of § 164.504(e).

Section 164.502(f)—Deceased Individuals

We proposed to extend privacy protections to the protected health information of a deceased individual for two years following the date of death. During the two-year time frame, we proposed in the definition of ''individual'' that the right to control the deceased individual's protected health information would be held by an executor or administrator, or other person (*e.g.*, next of kin) authorized under applicable law to act on behalf of the decedent's estate. The only proposed exception to this standard allowed for uses and disclosures of a decedent's protected health information for research purposes without the authorization of a legal representative and without the Institutional Review Board (IRB) or privacy board approval required (in proposed § 164.510(j)) for most other uses and disclosures for research.

In the final rule (§ 164.502(f)), we modify the standard to extend protection of protected health information about deceased individuals for as long as the covered entity maintains the information. We retain the exception for uses and disclosures for research purposes, now part of § 164.512(i), but also require that the

covered entity take certain verification measures prior to release of the decedent's protected health information for such purposes (see §§ 164.514(h) and 164.512(i)(1)(iii)).

We remove from the definition of ''individual'' the provision related to deceased persons. Instead, we create a standard for ''personal representatives'' (§ 164.502(g), see discussion below) that requires a covered entity to treat a personal representative of an individual as the individual in certain circumstances, *i.e.*, allows the representative to exercise the rights of the individual. With respect to deceased individuals, the final rule describes when a covered entity must allow a person who otherwise is permitted under applicable law to act with respect to the interest of the decedent or on behalf of the decedent's estate, to make decisions regarding the decedent's protected health information.

The final rule also adds a provision to § 164.512(g), that permits covered entities to disclose protected health information to a funeral director, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. Such disclosures are permitted both after death and in reasonable anticipation of death.

Section 164.502(g)—Personal Representatives

In the proposed rule we defined ''individual'' to include certain persons who were authorized to act on behalf of the person who is the subject of the protected health information. For adults and emancipated minors, the NPRM provided that ''individual'' includes a legal representative to the extent to which applicable law permits such legal representative to exercise the individual's rights in such contexts. With respect to unemancipated minors, we proposed that the definition of ''individual'' include a parent, guardian, or person acting *in loco parentis*, (hereinafter referred to as ''parent'') except when an unemancipated minor obtained health care services without the consent of, or notification to, a parent. Under the proposed rule, if a minor obtained health care services under these conditions, the minor would have had the exclusive rights of an individual with respect to the protected health information related to such health care services.

In the final rule, the definition of ''individual'' is limited to the subject of the protected health information, which includes unemancipated minors and other individuals who may lack capacity to act on their own behalf. We remove from the definition of ''individual'' the provisions regarding legal representatives. The circumstances in which a representative must be treated as an individual for purposes of this rule are addressed in a separate standard titled ''personal representatives.'' (§ 164.502(g)). The standard regarding personal representatives incorporates some changes to the proposed provisions regarding legal representatives. In general, under the final regulation, the ''personal representatives'' provisions are directed at the more formal representatives, while § 164.510(b) addresses situations in which persons are informally acting on behalf of an individual.

With respect to adults or emancipated minors, we clarify that a covered entity must treat a person as a personal representative of an individual if such person is, under applicable law, authorized to act on behalf of the individual in making decisions related to health care. This includes a court-appointed guardian and a person with a power of attorney, as set forth in the NPRM, but may also include other persons. The authority of a personal representative under this rule is limited: the representative must be treated as the individual only to the extent that protected health information is relevant to the matters on which the personal representative is authorized to represent the individual. For example, if a person's authority to make health care decisions for an individual is limited to decisions regarding treatment for cancer, such person is a personal representative and must be treated as the individual with respect to protected health information related to the cancer treatment of the individual. Such a person is not the personal representative of the individual with respect to all protected health information about the individual, and therefore, a covered entity may not disclose protected health information that is not relevant to the cancer treatment to the person, unless otherwise permitted under the rule. We intend this provision to apply to persons empowered under state or other law to make health related decisions for an individual, whether or not the instrument or law granting such authority specifically addresses health information.

In addition, we clarify that with respect to an unemancipated minor, if under applicable law a parent may act on behalf of an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this rule with respect to protected health information relevant to such personal representation, with three exceptions. Under the general rule, in most circumstances the minor would not have the capacity to act as the individual, and the parent would be able to exercise rights and authorities on behalf of the minor. Under the exceptions to the rule on personal representatives of unemancipated minors, the minor, and not the parent, would be treated as the individual and able to exercise the rights and authorities of an individual under the rule. These exceptions occur if: (1) The minor consents to a health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative; (2) the minor may lawfully obtain such health care service without the consent of a parent, and the minor, a court, or another person authorized by law consents to such health care service; or (3) a parent assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service. We note that the definition of health care includes services, but we use ''health care service'' in this provision to clarify that the scope of the rights of minors under this rule is limited to the protected health information related to a particular service.

Under this provision, we do not provide a minor with the authority to act under the rule unless the state has given them the ability to obtain health care without consent of a parent, or the parent has assented. In addition, we defer to state law where the state authorizes or prohibits disclosure of protected health information to a parent. See part 160, subpart B, Preemption of State Law. This rule does not affect parental notification laws that permit or require disclosure of protected health information to a parent. However, the rights of a minor under this rule are not otherwise affected by such notification.

In the final rule, the provision regarding personal representatives of deceased individuals has been changed to clarify the provision. The policy has not changed substantively from the NPRM.

Finally, we added a provision in the final rule to permit covered entities to elect not to treat a person as a personal representative in abusive situations. Under this provision, a covered entity need not treat a person as a personal representative of an individual if the covered entity, in the exercise of professional judgment, decides that it is

not in the best interest of the individual to treat the person as the individual's personal representative and the covered entity has a reasonable belief that the individual has been or may be subjected to domestic violence, abuse, or neglect by such person, or that treating such person as the personal representative could endanger the individual.

Section 164.502(g) requires a covered entity to treat a person that meets the requirements of a personal representative as the individual (with the exceptions described above). We note that disclosure of protected health information to a personal representative is mandatory under this rule only if disclosure to the individual is mandatory. Disclosure to the individual is mandatory only under §§ 164.524 and 164.528. Further, as noted above, the personal representative's rights are limited by the scope of its authority under other law. Thus, this provision does not constitute a general grant of authority to personal representatives.

We make disclosure to personal representatives mandatory to ensure that an individual's rights under §§ 164.524 and 164.528 are preserved even when individuals are incapacitated or otherwise unable to act for themselves to the same degree as other individuals. If the covered entity were to have the discretion to recognize a personal representative as the individual, there could be situations in which no one could invoke an individual's rights under these sections.

We continue to allow covered entities to use their discretion to disclose certain protected health information to family members, relatives, close friends, and other persons assisting in the care of an individual, in accordance with § 164.510(b). We recognize that many health care decisions take place on an informal basis, and we permit disclosures in certain circumstance to permit this practice to continue. Health care providers may continue to use their discretion to address these informal situations.

Section 164.502(h)—Confidential Communications

In the NPRM, we did not directly address the issue of whether an individual could request that a covered entity restrict the manner in which it communicated with the individual. The NPRM did provide individuals with the right to request that health care providers restrict uses and disclosures of protected health information for treatment, payment and health operations, but providers were not required to agree to such a restriction.

In the final rule, we require covered providers to accommodate reasonable requests by patients about how the covered provider communicates with the individual. For example, an individual who does not want his or her family members to know about a certain treatment may request that the provider communicate with the individual at his or her place of employment, or to send communications to a designated address. Covered providers must accommodate the request unless it is unreasonable. Similarly, the final rule permits individuals to request that health plans communicate with them by alternative means, and the health plan must accommodate such a request if it is reasonable and the individual states that disclosure of the information could endanger the individual. The specific provisions relating to confidential communications are in § 164.522.

Section 164.502(i)—Uses and Disclosures Consistent with Notice

We proposed to prohibit covered entities from using or disclosing protected health information in a manner inconsistent with their notice of information practices. We retain this provision in the final rule. See § 164.520 regarding notice content and distribution requirements.

Section 164.502(j)—Disclosures by Whistleblowers and Workforce Member Crime Victims

Disclosures by Whistleblowers

In § 164.518(c)(4) of the NPRM we addressed the issue of whistleblowers by proposing that a covered entity not be held in violation of this rule because a member of its workforce or a person associated with a business associate of the covered entity used or disclosed protected health information that such person believed was evidence of a civil or criminal violation, and any disclosure was: (1) Made to relevant oversight agencies or law enforcement or (2) made to an attorney to allow the attorney to determine whether a violation of criminal or civil law had occurred or to assess the remedies or actions at law that may be available to the person disclosing the information.

We included an extensive discussion on how whistleblower actions can further the public interest, including reference to the need in some circumstances to utilize protected health information for this purpose as well as reference to the *qui tam* provisions of the Federal False Claims Act.

In the final rule we retitle the provision and include it in § 164.502 to reflect the fact that these disclosures are not made by the covered entity and therefore this material does not belong in the section on safeguarding information against disclosure.

We retain the basic concept in the NPRM of providing protection to a covered entity for the good faith whistleblower action of a member of its workforce or a business associate. We clarify that a whistleblower disclosure by an employee, subcontractor, or other person associated with a business associate is considered a whistleblower disclosure of the business associate under this provision. However, in the final rule, we modify the scope of circumstances under which a covered entity is protected in whistleblower situations. A covered entity is not in violation of the requirements of this rule when a member of its workforce or a business associate of the covered entity discloses protected health information to: (i) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity; (ii) an appropriate health care accreditation organization; or (iii) an attorney, for the purpose of determining his or her legal options with respect to whistleblowing. We delete disclosures to a law enforcement official.

We expand the scope of this section to cover disclosures of protected health information to an oversight or accreditation organization for the purpose of reporting breaches of professional standards or problems with quality of care. The covered entity will not be in violation of this rule, provided that the disclosing individual believes in good faith that the covered entity has engaged in conduct which is unlawful or otherwise violates professional or clinical standards, or that the care, services or conditions provided by the covered entity potentially endanger one or more patients, workers or the public. Since these provisions only relate to whistleblower actions in relation to the covered entity, disclosure of protected health information to expose malfeasant conduct by another person, such as knowledge gained during the course of treatment about an individual's illicit drug use, would not be protected activity.

We clarify that this section only applies to protection of a covered entity, based on the whistleblower action of a member of its workforce or business associates. Since the HIPAA legislation only applies to covered entities, not their workforces, it is beyond the scope of this rule to directly regulate the

whistleblower actions of members of a covered entity's workforce.

In the NPRM, we had proposed to require covered entities to apply sanctions to members of its workforce who improperly disclose protected health information. In this final rule, we retain this requirement in § 164.530(e)(1) but modify the proposed provision on sanctions to clarify that the sanctions required under this rule do not apply to workforce members of a covered entity for whistleblower disclosures.

Disclosures by Workforce Members Who Are Crime Victims

The proposed rule did not address disclosures by workforce members who are victims of a crime. In the final rule, we clarify that a covered entity is not in violation of the rule when a workforce member of a covered entity who is the victim of a crime discloses protected health information to law enforcement officials about the suspected perpetrator of the crime. We limit the amount of protected health information that may be disclosed to the limited information for identification and location described in § 164.512(f)(2).

We note that this provision is similar to the provision in § 164.512(f)(5), which permits a covered entity to disclose protected health information to law enforcement that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity. This provision differs in that it permits the disclosure even if the crime occurred somewhere other than on the premises of the covered entity. For example, if a hospital employee is the victim of an attack outside of the hospital, but spots the perpetrator sometime later when the perpetrator seeks medical care at the hospital, the workforce member who was attacked may notify law enforcement of the perpetrator's location and other identifying information. We do not permit, however, the disclosure of protected health information other than that described in § 164.512(f)(2).

Section 164.504—Uses and Disclosures—Organizational Requirements—Component Entities, Affiliated Entities, Business Associates and Group Health Plans

Section 164.504(a)–(c)—Health Care Component (Component Entities)

In the preamble to the proposed rule we introduced the concept of a ''component entity'' to differentiate the health care unit of a larger organization from the larger organization. In the proposal we noted that some organizations that are primarily involved in non-health care activities do provide health care services or operate health plans or health care clearinghouses. Examples included a school with an on-site health clinic and an employer that self administers a sponsored health plan. In such cases, the proposal said that the health care component of the entity would be considered the covered entity, and any release of information from that component to another office or person in the organization would be a regulated disclosure. We would have required such entities to create barriers to prevent protected health information from being used or disclosed for activities not authorized or permitted under the proposal.

We discuss group health plans and their relationships with plan sponsors below under ''Requirements for Group Health Plans.''

In the final rule we address the issue of differentiating health plan, covered health care provider and health care clearinghouse activities from other functions carried out by a single legal entity in paragraphs (a)–(c) of § 164.504. We have created a new term, ''hybrid entity'', to describe the situation where a health plan, health care provider, or health care clearinghouse is part of a larger legal entity; under the definition, a ''hybrid entity'' is ''a single legal entity that is a covered entity and whose covered functions are not its primary functions.'' The term ''covered functions'' is discussed above under § 164.501. By ''single legal entity'' we mean a legal entity, such as a corporation or partnership, that cannot be further differentiated into units with their own legal identities. For example, for purposes of this rule a multinational corporation composed of multiple subsidiary companies would not be a single legal entity, but a small manufacturing firm and its health clinic, if not separately incorporated, could be a single legal entity.

The health care component rules are designed for the situation in which the health care functions of the legal entity are not its dominant mission. Because some part of the legal entity meets the definition of a health plan or other covered entity, the legal entity as a whole could be required to comply with the rules below. However, in such a situation, it makes sense not to require the entire entity to comply with the requirements of the rules below, when most of its activities may have little or nothing to do with the provision of health care; rather, as a practical matter, it makes sense for such an entity to focus its compliance efforts on the component that is actually performing the health care functions. On the other hand, where most of what the covered entity does consist of covered functions, it makes sense to require the entity as a whole to comply with the rules. The provisions at §§ 164.504(a)–(c) provide that for a hybrid entity, the rules apply only to the part of the entity that is the health care component. At the same time, the lack of corporate boundaries increases the risk that protected health information will be used in a manner that would not otherwise be permitted by these rules. Thus, we require that the covered entity erect firewalls to protect against the improper use or disclosure within or by the organization. See § 164.504(c)(2).

The term ''primary functions'' in the definition of ''hybrid entity'' is not meant to operate with mathematical precision. Rather, we intend that a more common sense evaluation take place: Is most of what the covered entity does related to its health care functions? If so, then the whole entity should be covered. Entities with different insurance lines, if not separately incorporated, present a particular issue with respect to this analysis. Because the definition of ''health plan'' excludes many types of insurance products (in the exclusion under paragraph (2)(i) of the definition), we would consider an entity that has one or more of these lines of insurance in addition to its health insurance lines to come within the definition of ''hybrid entity,'' because the other lines of business constitute substantial parts of the total business operation and are required to be separate from the health plan(s) part of the business.

An issue that arises in the hybrid entity situation is what records are covered in the case of an office of the hybrid entity that performs support functions for both the health care component of the entity and for the rest of the entity. For example, this situation could arise in the context of a company with an onsite clinic (which we will assume is a covered health care provider), where the company's business office maintains both clinic records and the company's personnel records. Under the definition of the term ''health care component,'' the business office is part of the health care component (in this hypothetical, the clinic) ''to the extent that'' it is performing covered functions on behalf of the clinic involving the use or disclosure of protected health information that it receives from, creates or maintains for the clinic. Part of the business office, therefore, is part of the

health care component, and part of the business office is outside the health care component. This means that the non-health care component part of the business office is not covered by the rules below. Under our hypothetical, then, the business office would not be required to handle its personnel records in accordance with the rules below. The hybrid entity would be required to establish firewalls with respect to these record systems, to ensure that the clinic records were handled in accordance with the rules.

With respect to excepted benefits, the rules below operate as follows. (Excepted benefits include accident, disability income, liability, workers' compensation and automobile medical payment insurance.) Excepted benefit programs are excluded from the health care component (or components) through the definition of ''health plan.'' If a particular organizational unit performs both excepted benefits functions and covered functions, the activities associated with the excepted benefits program may not be part of the health care component. For example, an accountant who works for a covered entity with both a health plan and a life insurer would have his or her accounting functions performed for the health plan as part of the component, but not the life insurance accounting function. See § 164.504(c)(2)(iii). We require this segregation of excepted benefits because HIPAA does not cover such programs, policies and plans, and we do not permit any use or disclosure of protected health information for the purposes of operating or performing the functions of the excepted benefits without authorization from the individual, except as otherwise permitted in this rule.

In § 164.504(c)(2) we require covered entities with a health care component to establish safeguard policies and procedures to prevent any access to protected health information by its other organizational units that would not be otherwise permitted by this rule. We note that section 1173(d)(1)(B) of HIPAA requires policies and procedures to isolate the activities of a health care clearinghouse from a ''larger organization'' to prevent unauthorized access by the larger organization. This safeguard provision is consistent with the statutory requirement and extends to any covered entity that performs ''non-covered entity functions'' or operates or conducts functions of more than one type of covered entity.

Because, as noted, the covered entity in the hybrid entity situation is the legal entity itself, we state explicitly what is implicitly the case, that the covered entity (legal entity) remains responsible for compliance vis-a-vis subpart C of part 160. See § 164.504(c)(3)(i). We do this simply to make these responsibilities clear and to avoid confusion on this point. Also, in the hybrid entity situation the covered entity/legal entity has control over the entire workforce, not just the workforce of the health care component. Thus, the covered entity is in a position to implement policies and procedures to ensure that the part of its workforce that is doing mixed or non-covered functions does not impermissibly use or disclose protected health information. Its responsibility to do so is clarified in § 164.504(c)(3)(ii).

Section 164.504(d)—Affiliated Entities

Some legally distinct covered entities may share common administration of organizationally differentiated but similar activities (for example, a hospital chain). In § 164.504(d) we permit legally distinct covered entities that share common ownership or control to designate themselves, or their health care components, together to be a single covered entity. Common control exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity. Common ownership exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity.

Such organizations may promulgate a single shared notice of information practices and a consent form. For example, a corporation with hospitals in twenty states may designate itself as a covered entity and, therefore, able to merge information for joint marketplace analyses. The requirements that apply to a covered entity also apply to an affiliated covered entity. For example, under the minimum necessary provisions, a hospital in one state could not share protected health information about a particular patient with another hospital if such a use is not necessary for treatment, payment or health care operations. The covered entities that together make up the affiliated covered entity are separately subject to liability under this rule. The safeguarding requirements for affiliated covered entities track the requirements that apply to health care components.

Section 164.504(e)—Business Associates

In the NPRM, we proposed to require a contract between a covered entity and a business associate, except for disclosures of protected health information by a covered entity that is a health care provider to another health care provider for the purposes of consultation or referral. A covered entity would have been in violation of this rule if the covered entity knew or reasonably should have known of a material breach of the contract by a business associate and it failed to take reasonable steps to cure the breach or terminate the contract. We proposed in the preamble that when a covered entity acted as a business associate to another covered entity, the covered entity that was acting as business associate also would have been responsible for any violations of the regulation.

We also proposed that covered health care providers receiving protected health information for consultation or referral purposes would still have been subject to this rule, and could not have used or disclosed such protected health information for a purpose other than the purpose for which it was received (*i.e.,* the consultation or referral). Further, we noted that providers making disclosures for consultations or referrals should be careful to inform the receiving provider of any special limitations or conditions to which the disclosing provider had agreed to impose (*e.g.,* the disclosing provider had provided notice to its patients that it would not make disclosures for research).

We proposed that business associates would not have been permitted to use or disclose protected health information in ways that would not have been permitted of the covered entity itself under these rules, and covered entities would have been required to take reasonable steps to ensure that protected health information disclosed to a business associate remained protected.

In the NPRM (proposed § 164.506(e)(2)) we would have required that the contractual agreement between a covered entity and a business associate be in writing and contain provisions that would:

- Prohibit the business associate from further using or disclosing the protected health information for any purpose other than the purpose stated in the contract.
- Prohibit the business associate from further using or disclosing the protected health information in a manner that would violate the requirements of this proposed rule if it were done by the covered entity.
- Require the business associate to maintain safeguards as necessary to ensure that the protected health information is not used or disclosed except as provided by the contract.
- Require the business associate to report to the covered entity any use or disclosure of the protected health information of which the business

associate becomes aware that is not provided for in the contract.

- Require the business associate to ensure that any subcontractors or agents to whom it provides protected health information received from the covered entity will agree to the same restrictions and conditions that apply to the business associate with respect to such information.
- Require the business associate to provide access to non-duplicative protected health information to the subject of that information, in accordance with proposed § 164.514(a).
- Require the business associate to make available its internal practices, books and records relating to the use and disclosure of protected health information received from the covered entity to the Secretary for the purposes of enforcing the provisions of this rule.
- Require the business associate, at termination of the contract, to return or destroy all protected health information received from the covered entity that the business associate still maintains in any form to the covered entity and prohibit the business associate from retaining such protected health information in any form.
- Require the business associate to incorporate any amendments or corrections to protected health information when notified by the covered entity that the information is inaccurate or incomplete.
- State that individuals who are the subject of the protected health information disclosed are intended to be third party beneficiaries of the contract.
- Authorize the covered entity to terminate the contract, if the covered entity determines that the business associate has violated a material term of the contract.

We also stated in the preamble to the NPRM that the contract could have included any additional arrangements that did not violate the provisions of this regulation.

We explained in the preamble to the NPRM that a business associate (including business associates that are covered entities) that had contracts with more than one covered entity would have had no authority to combine, aggregate or otherwise use for a single purpose protected health information obtained from more than one covered entity unless doing so would have been a lawful use or disclosure for each of the covered entities that supplied the protected health information that is being combined, aggregated or used. In addition, the business associate would have had to have been authorized through the contract or arrangement with each covered entity that supplied the protected health information to combine or aggregate the information. A covered entity would not have been permitted to obtain protected health information through a business associate that it could not otherwise obtain itself.

In the final rule we retain the overall approach proposed: covered entities may disclose protected health information to persons that meet the rule's definition of business associate, or hire such persons to obtain or create protected health information for them, only if covered entities obtain specified satisfactory assurances from the business associate that it will appropriately handle the information; the regulation specifies the elements of such satisfactory assurances; covered entities have responsibilities when such specified satisfactory assurances are violated by the business associate. We retain the requirement that specified satisfactory assurances must be obtained if a covered entity's business associate is also a covered entity. We note that a master business associate contract or MOU that otherwise meets the requirements regarding specified satisfactory assurances meets the requirements with respect to all the signatories.

A covered entity may disclose protected health information to a business associate, consistent with the other requirements of the final rule, as necessary to permit the business associate to perform functions and activities for or on behalf of the covered entity, or to provide the services specified in the business associate definition to or for the covered entity. As discussed below, a business associate may only use the protected health information it receives in its capacity as a business associate to a covered entity as permitted by its contract or agreement with the covered entity.

We do not attempt to directly regulate business associates, but pursuant to our authority to regulate covered entities we place restrictions on the flow of information from covered entities to non-covered entities. We add a provision to clarify that a violation of a business associate agreement by a covered entity that is a business associate of another covered entity constitutes a violation of this rule.

In the final rule, we make significant changes to the requirements regarding business associates. As explained below in more detail: we make significant changes to the content of the required contractual satisfactory assurances; we include exceptions for arrangements that would otherwise meet the definition of business associate; we make special provisions for government agencies that by law cannot enter into contracts with one another or that operate under other legal requirements incompatible with some aspects of the required contractual satisfactory assurances; we provide a new mechanism for covered entities to hire a third party to aggregate data.

The final rule provides several exception to the business associate requirements, where a business associate relationship would otherwise exist. We substantially expand the exception for disclosure of protected health information for treatment. Rather than allowing disclosures without business associate assurances only for the purpose of consultation or referral, in the final rule we allow covered entities to make any disclosure of protected health information for treatment purposes to a health care provider without a business associate arrangement. This provision includes all activities that fall under the definition of treatment.

We do not require a business associate contract for a group health plan to make disclosures to the plan sponsor, to the extent that the health plan meets the applicable requirements of § 164.504(f).

We also include an exception for certain jointly administered government programs providing public benefits. Where a health plan that is a government program provides public benefits, such as SCHIP and Medicaid, and where eligibility for, or enrollment in, the health plan is determined by an agency other than the agency administering the health plan, or where the protected health information used to determine enrollment or eligibility in the health plan is collected by an agency other than the agency administering the health plan, and the joint activities are authorized by law, no business associate contract is required with respect to the collection and sharing of individually identifiable health information for the performance of the authorized functions by the health plan and the agency other than the agency administering the health plan. We note that the phrase ''government programs providing public benefits'' refers to programs offering benefits to specified members of the public and not to programs that offer benefits only to employees or retirees of government agencies.

We note that we do not consider a financial institution to be acting on behalf of a covered entity, and therefore no business associate contract is required, when it processes consumer-conducted financial transactions by debit, credit or other payment card,

clears checks, initiates or processes electronic funds transfers, or conducts any other activity that directly facilitates or effects the transfer of funds for compensation for health care. A typical consumer-conducted payment transaction is when a consumer pays for health care or health insurance premiums using a check or credit card. In these cases, the identity of the consumer is always included and some health information (*e.g.,* diagnosis or procedure) may be implied through the name of the health care provider or health plan being paid. Covered entities that initiate such payment activities must meet the minimum necessary disclosure requirements described in the preamble to § 164.514.

In the final rule, we reduce the extent to which a covered entity must monitor the actions of its business associate and we make it easier for covered entities to identify the circumstances that will require them to take actions to correct a business associate's material violation of the contract, in the following ways. We delete the proposed language requiring covered entities to ''take reasonable steps to ensure'' that each business associate complies with the rule's requirements. Additionally, we now require covered entities to take reasonable steps to cure a breach or terminate the contract for business associate behaviors only if they know of a material violation by a business associate. In implementing this standard, we will view a covered entity that has substantial and credible evidence of a violation as knowing of such violation. While this standard relieves the covered entity of the need to actively monitor its business associates, a covered entity nonetheless is expected to investigate when they receive complaints or other information that contain substantial and credible evidence of violations by a business associate, and it must act upon any knowledge of such violation that it possesses. We note that a whistleblowing disclosure by a business associate of a covered entity that meets the requirements of § 164.502(j)(1) does not put the covered entity in violation of this rule, and the covered entity has no duty to correct or cure, or to terminate the relationship.

We also qualify the requirement for terminating contracts with non-compliant business associates. The final rule still requires that the business associate contract authorize the covered entity to terminate the contract, if the covered entity determines that the business associate has violated a material term of the contract, and it requires the covered entity to terminate the contract if steps to cure such a material breach fail. The rule now stipulates, however, that if the covered entity is unable to cure a material breach of the business associate's obligation under the contract, it is expected to terminate the contract, when feasible. This qualification has been added to accommodate circumstances where terminating the contract would be unreasonably burdensome on the covered entity, such as when there are no viable alternatives to continuing a contract with that particular business associate. It does not mean, for instance, that the covered entity can choose to continue the contract with a non-compliant business associate merely because it is more convenient or less costly than contracts with other potential business associates. We also require that if a covered entity determines that it is not feasible to terminate a non-compliant business associate, the covered entity must notify the Secretary.

We retain all of the requirements for a business associate contract that were listed in proposed § 164.506(e)(2), with some modifications. See § 164.504(e)(2).

We retain the requirement that the business associate contract must provide that the business associate will not use or further disclose the information other than as permitted or required by the contract or as required by law. We do not mean by this requirement that the business associate contract must specify each and every use and disclosure of protected health information permitted to the business associate. Rather, the contract must state the purposes for which the business associate may use and disclose protected health information, and must indicate generally the reasons and types of persons to whom the business associate may make further disclosures. For example, attorneys often need to provide information to potential witnesses, opposing counsel, and others in the course of their representation of a client. The business associate contract pursuant to which protected health information is provided to its attorney may include a general statement permitting the attorney to disclose protected health information to these types of people, within the scope of its representation of the covered entity.

We retain the requirement that a business associate contract may not authorize a business associate to use or further disclose protected health information in a manner that would violate the requirements of this subpart if done by the covered entity, but we add two exceptions. First, we permit a covered entity to authorize a business associate to use and disclose protected health information it receives in its capacity as a business associate for its proper management and administration and to carry out its legal responsibilities. The contract must limit further disclosures of the protected health information for these purposes to those that are required by law and to those for which the business associate obtains reasonable assurances that the protected health information will be held confidentially and that it will be notified by the person to whom it discloses the protected health information of any breaches of confidentiality.

Second, we permit a covered entity to authorize the business associate to provide data aggregation services to the covered entity. As discussed above in § 164.501, data aggregation, with respect to protected health information received by a business associate in its capacity as the business associate of a covered entity, is the combining of such protected health information by the business associate with protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit the creation of data for analyses that relate to the health care operations of the respective covered entities. We added this service to the business associate definition to clarify the ability of covered entities to contract with business associates to undertake quality assurance and comparative analyses that involve the protected health information of more than one contracting covered entity. We except data aggregation from the general requirement that a business associate contract may not authorize a business associate to use or further disclose protected health information in a manner that would violate the requirements of this subpart if done by the covered entity in order to permit the combining or aggregation of protected health information received in its capacity as a business associate of different covered entities when it is performing this service. In many cases, the combining of this information for the respective health care operations of the covered entities is not something that the covered entities could do—a covered entity cannot generally disclose protected health information to another covered entity for the disclosing covered entity's health care operations. However, we permit covered entities that enter into business associate contracts with a business associate for data aggregation to permit the business associate to combine or aggregate the protected health information they

disclose to the business associate for their respective health care operations.

We note that there may be other instances in which a business associate may combine or aggregate protected health information received in its capacity as a business associate of different covered entities, such as when it is performing health care operations on behalf of covered entities that participate in an organized health care arrangement. A business associate that is performing payment functions on behalf of different covered entities also may combine protected health information when it is necessary, such as when the covered entities share financial risk or otherwise jointly bill for services.

In the final rule we clarify that the business associate contract must require the business associate to make available protected health information for amendment and to incorporate such amendments. The business associate contract must also require the business associate to make available the information required to provide an accounting of disclosures. We provide more flexibility to the requirement that all protected health information be returned by the business associate upon termination of the contract. The rule now stipulates that if feasible, the protected health information should be destroyed or returned at the end of a contract. Accordingly, a contract with a business associate must state that if there are reasons that the return or destruction of the information is not feasible and the information must be retained for specific reasons and uses, such as for future audits, privacy protections must continue after the contract ends, for as long as the business associate retains the information. The contract also must state that the uses of information after termination of the contract must be limited to the specific set of uses or disclosures that make it necessary for the business associate to retain the information.

We also remove the requirement that business associate contracts contain a provision stating that individuals whose protected health information is disclosed under the contract are intended third-party beneficiaries of the contract. Third party beneficiary or similar responsibilities may arise under these business associate arrangements by operation of state law; we do not intend in this rule to affect the operation of such state laws.

We modify the requirement that a business associate contract require the business associate to ensure that agents abide by the provisions of the business associate contract. We clarify that agents includes subcontractors, and we note that a business associate contract must make the business associate responsible for ensuring that any person to whom it delegates a function, activity or service which is within its business associate contract with the covered entity agrees to abide by the restrictions and conditions that apply to the business associate under the contract. We note that a business associate will need to consider the purpose for which protected health information is being disclosed in determining whether the recipient must be bound to the restrictions and conditions of the business associate contract. When the disclosure is a delegation of a function, activity or service that the business associate has agreed to perform for a covered entity, the recipient who undertakes such a function steps into the shoes of the business associate and must be bound to the restrictions and conditions. When the disclosure is to a third party who is not performing business associate functions, activities or services for on behalf of the covered entity, but is the type of disclosure that the covered entity itself could make without giving rise to a business associate relationship, the business associate is not required to ensure that the restrictions or conditions of the business associate contract are maintained.

For example, if a business associate acts as the billing agent of a health care provider, and discloses protected health information on behalf of the hospital to health plans, the business associate has no responsibility with respect to further uses or disclosures by the health plan. In the example above, where a covered entity has a business associate contract with a lawyer, and the lawyer discloses protected health information to an expert witness in preparation for litigation, the lawyer again would have no responsibility under this subpart with respect to uses or disclosures by the expert witness, because such witness is not undertaking the functions, activities or services that the business associate lawyer has agreed to perform. However, if a covered entity contracts with a third party administrator to provide claims management, and the administrator delegates management of the pharmacy benefits to a third party, the business associate third party administrator must ensure that the pharmacy manager abides by the restrictions and conditions in the business associate contract between the covered entity and the third party administrator.

We provide in § 164.504(c)(3) several methods other than a business associate contract that will satisfy the requirement for satisfactory assurances under this section. First, when a government agency is a business associate of another government agency that is a covered entity, we permit memorandum of understanding between the agencies to constitute satisfactory assurance for the purposes of this rule, if the memorandum accomplishes each of the objectives of the business associate contract. We recognize that the relationships of government agencies are often organized as a matter of law, and that it is not always feasible for one agency to contract with another for all of the purposes provided for in this section. We also recognize that it may be incorrect to view one government agency as ''acting on behalf of'' the other government agency; under law, each agency may be acting to fulfill a statutory mission. We note that in some instances, it may not be possible for the agencies to include the right to terminate the arrangement because the relationship may be established under law. In such instances, the covered entity government agency would need to fulfill the requirement to report known violations of the memorandum to the Secretary.

Where the covered entity is a government agency, we consider the satisfactory assurances requirement to be satisfied if other law contains requirements applicable to the business associate that accomplish each of the objectives of the business associate contract. We recognize that in some cases, covered entities that are government agencies may be able to impose the requirements of this section directly on the persons acting as their business associates. We also recognize that often one government agency is acting as a business associate of another government agency, and either party may have the legal authority to establish the requirements of this section by regulation. We believe that imposing these requirements directly on business associates provides greater protection than we can otherwise provide under this section, and so we recognize such other laws as sufficient to substitute for a business associate contract.

We also recognize that there may be some circumstances where the relationship between covered entities and business associates is otherwise mandated by law. In the final rule, we provide that where a business associate is required by law to act as a business associate to a covered entity, the covered entity may disclose protected health information to the business associate to the extent necessary to comply with the legal mandate without

meeting the requirement to have a business associate contract (or, in the case of government agencies, a memorandum of understanding or law pertaining to the business associate) if it makes a good faith attempt the obtain satisfactory assurances required by this section and, if unable to do so, documents the attempt and the reasons that such assurances cannot be obtained. This provision addresses situations where law requires one party to act as the business associate of another party. The fact that the parties have contractual obligations that may be enforceable is not sufficient to meet the required by law test in this provision.

This provision recognizes that in some instances the law requires that a government agency act as a business associate of a covered entity. For example, the United States Department of Justice is required by law to defend tort suits brought against certain covered entities; in such circumstances, however, the United States, and not the individual covered entity, is the client and is potentially liable. In such situations, covered entities must be able to disclose protected health information needed to carry out the representation, but the particular requirements that would otherwise apply to a business associate relationship may not be possible to obtain. Subsection (iii) makes clear that, where the relationship is required by law, the covered entity complies with the rule if it attempts, in good faith, to obtain satisfactory assurances as are required by this paragraph and, if such attempt fails, documents the attempts and the reasons that such assurances cannot be obtained.

The operation of the final rule maintains the construction discussed in the preamble to the NPRM that a business associate (including a business associate that is a covered entity) that has business associate contracts with more than one covered entity generally may not use or disclose the protected health information that it creates or receives in its capacity as a business associate of one covered entity for the purposes of carrying out its responsibilities as a business associate of another covered entity, unless doing so would be a lawful use or disclosure for each of the covered entities and the business associate's contract with each of the covered entities permits the business associate to undertake the activity. For example, a business associate performing a function under health care operations on behalf of an organized health care arrangement would be permitted to combine or aggregate the protected health information obtained from covered entities participating in the arrangement to the extent necessary to carry out the authorized activity and in conformance with its business associate contracts. As described above, a business associate providing data aggregation services to different covered entities also could combine and use the protected health information of the covered entities to assist with their respective health care operations. A covered entity that is undertaking payment activities on behalf of different covered entities also may use or disclose protected health information obtained as a business associate of one covered entity when undertaking such activities as a business associate of another covered entity where the covered entities have authorized the activities and where they are necessary to secure payment for the entities. For example, when a group of providers share financial risk and contract with a business associate to conduct payment activities on their behalf, the business associate may use the protected health information received from the covered entities to assist them in managing their shared risk arrangement.

Finally, we note that the requirements imposed by this provision are intended to extend privacy protection to situations in which a covered entity discloses substantial amounts of protected health information to other persons so that those persons can perform functions or activities on its behalf or deliver specified services to it. A business associate contract basically requires the business associate to maintain the confidentiality of the protected health information that it receives and generally to use and disclose such information for the purposes for which it was provided. This requirement does not interfere with the relationship between a covered entity and business associate, or require the business associate to subordinate its professional judgment to that of a covered entity. Covered entities may rely on the professional judgment of their business associates as to the type and amount of protected health information that is necessary to carry out a permitted activity. The requirements of this provision are aimed at securing the continued confidentiality of protected health information disclosed to third parties that are serving the covered entity's interests.

Section 164.504(f)—Group Health Plans

Covered entities under HIPAA include health care clearinghouses, health care providers and health plans. Specifically included in the definition of ''health plan'' are group health plans (as defined in section 2791(a) of the Public Health Service Act) with 50 or more participants or those of any size that are administered by an entity other than the employer who established and maintains the plan. These group health plans may be fully insured or self-insured. Neither employers nor other group health plan sponsors are defined as covered entities. However, employers and other plan sponsors—particularly those sponsors with self-insured group health plans—may perform certain functions that are integrally related to or similar to the functions of group health plans and, in carrying out these functions, often require access to individual health information held by the group health plan.

Most group health plans are also regulated under the Employee Retirement Income Security Act of 1974 (ERISA). Under ERISA, a group health plan must be a separate legal entity from its plan sponsor. ERISA-covered group health plans usually do not have a corporate presence, in other words, they may not have their own employees and sometimes do not have their own assets (*i.e.,* they may be fully insured or the benefits may be funded through the general assets of the plan sponsor, rather than through a trust). Often, the only tangible evidence of the existence of a group health plan is the contractual agreement that describes the rights and responsibilities of covered participants, including the benefits that are offered and the eligible recipients.

ERISA requires the group health plan to identify a ''named fiduciary,'' a person responsible for ensuring that the plan is operated and administered properly and with ultimate legal responsibility for the plan. If the plan documents under which the group health plan was established and is maintained permit, the named fiduciary may delegate certain responsibilities to trustees and may hire advisors to assist it in carrying out its functions. While generally the named fiduciary is an individual, it may be another entity. The plan sponsor or employees of the plan sponsor are often the named fiduciaries. These structural and operational relationships present a problem in our ability to protect health information from being used inappropriately in employment-related decisions. On the one hand, the group health plan, and any health insurance issuer or HMO providing health insurance or health coverage to the group health plan, are covered entities under the regulation and may only disclose protected health information as authorized under the

regulation or with individual consent. On the other hand, plan sponsors may need access to protected health information to carry out administration functions on behalf of the plan, but under circumstances in which securing individual consent is impractical. We note that we sometimes refer in the rule and preamble to health insurance issuers and HMOs that provide health insurance or health coverage to a group health plan as health insurance issuers or HMOs with respect to a group health plan.

The proposed rule used the health care component approach for employers and other plan sponsors. Under this approach, only the component of an employer or other plan sponsor would be treated as a covered entity. The component of the plan sponsor would have been able to use protected health information for treatment, payment, and health care operations, but not for other purposes, such as discipline, hiring and firing, placement and promotions. We have modified the final rule in a number of ways.

In the final rule, we recognize plan sponsors' legitimate need for health information in certain situations while, at the same time, protecting health information from being used for employment-related functions or for other functions related to other employee benefit plans or other benefits provided by the plan sponsor. We do not attempt to directly regulate employers or other plan sponsors, but pursuant to our authority to regulate health plans, we place restrictions on the flow of information from covered entities to non-covered entities.

The final rule permits group health plans, and allows them to authorize health insurance issuers or HMOs with respect to the group health plan, to disclose protected health information to plan sponsors if the plan sponsors voluntarily agree to use and disclose the information only as permitted or required by the regulation. The information may be used only for plan administration functions performed on behalf of the group health plan which are specified in plan documents. The group health plan is not required to have a business associate contract with the plan sponsor to disclose the protected health information or allow the plan sponsor to create protected health information on its behalf, if the conditions of § 164.504(e) are met.

In order for the group health plan to disclose protected health information to a plan sponsor, the plan documents under which the plan was established and is maintained must be amended to: (1) Describe the permitted uses and disclosures of protected health information; (2) specify that disclosure is permitted only upon receipt of a certification from the plan sponsor that the plan documents have been amended and the plan sponsor has agreed to certain conditions regarding the use and disclosure of protected health information; and (3) provide adequate firewalls to: identify the employees or classes of employees who will have access to protected health information; restrict access solely to the employees identified and only for the functions performed on behalf of the group health plan; and provide a mechanism for resolving issues of noncompliance.

Any employee of the plan sponsor who receives protected health information for payment, health care operations or other matters related to the group health plan must be identified in the plan documents either by name or function. We assume that since individuals employed by the plan sponsor may change frequently, the group health plan would likely describe such individuals in a general manner. Any disclosure to employees or classes of employees not identified in the plan documents is not a permissible disclosure. To the extent a group health plan does have its own employees separate from the plan sponsor's employees, as the workforce of a covered entity (*i.e.* the group health plan), they also are bound by the permitted uses and disclosures of this rule.

The certification that must be given to the group health plan must state that the plan sponsor agrees to: (1) Not use or further disclose protected health information other than as permitted or required by the plan documents or as required by law; (2) ensure that any subcontractors or agents to whom the plan sponsor provides protected health information agree to the same restrictions; (3) not use or disclose the protected health information for employment-related actions; (4) report to the group health plan any use or disclosure that is inconsistent with the plan documents or this regulation; (5) make the protected health information accessible to individuals; (6) allow individuals to amend their information; (7) provide an accounting of its disclosures; (8) make its practices available to the Secretary for determining compliance; (9) return and destroy all protected health information when no longer needed, if feasible; and (10) ensure that the firewalls have been established.

We have included this certification requirement in part, as a way to reduce the burden on health insurance issuers and HMOs. Without a certification, health insurance issuers and HMOs would need to review the plan documents in order to ensure that the amendments have been made before they could disclose protected health information to plan sponsors. The certification, however, is a simple statement that the amendments have been made and that the plan sponsor has agreed to certain restrictions on the use and disclosure of protected health information. The receipt of the certification therefore, is sufficient basis for the health insurance issuer or HMO to disclose protected health information to the plan sponsor.

Many activities included in the definitions of health care operations and payment are commonly referred to as plan administration functions in the ERISA group health plan context. For purposes of this rule, plan administration activities are limited to activities that would meet the definition of payment or health care operations, but do not include functions to modify, amend, or terminate the plan or solicit bids from prospective issuers. Plan administration functions include quality assurance, claims processing, auditing, monitoring, and management of carve-out plans—such as vision and dental. Under the final rule, ''plan administration'' does not include any employment-related functions or functions in connection with any other benefits or benefit plans, and group health plans may not disclose information for such purposes absent an authorization from the individual. For purposes of this rule, enrollment functions performed by the plan sponsor on behalf of its employees are not considered plan administration functions.

Plan sponsors have access to protected health information only to the extent group health plans have access to protected health information and plan sponsors are permitted to use or disclose protected health information only as would be permitted by group health plans. That is, a group health plan may permit a plan sponsor to have access to or to use protected health information only for purposes allowed by the regulation.

As explained above, where a group health plan purchases insurance or coverage from a health insurance issuer or HMO, the provision of insurance or coverage by the health insurance issuer or HMO to the group health plan does not make the health insurance issuer or HMO a business associate. In such case, the activities of the health insurance issuer or HMO are on their own behalf and not on the behalf of the group

health plan. We note that where a group health plan contracts with a health insurance issuer or HMO to perform functions or activities or to provide services that are in addition to or not directly related to the provision of insurance, the health insurance issuer or HMO may be a business associate with respect to those additional functions, activities, or services. In addition, group health plans that provide health benefits only through an insurance contract and do not create, maintain, or receive protected health information (except for summary information described below or information that merely states whether an individual is enrolled in or has been disenrolled from the plan) do not have to meet the notice requirements of § 164.520 or the administrative requirements of § 164.530, except for the documentation requirement in § 164.530(j), because these requirements are satisfied by the issuer or HMO that is providing benefits under the group health plan. A group health plan, however, may not permit a health insurance issuer or HMO to disclose protected health information to a plan sponsor unless the notice required in 164.520 indicate such disclosure may occur.

The final rule also permits a health plan that is providing insurance to a group health plan to provide summary information to the plan sponsor to permit the plan sponsor to solicit premium bids from other health plans or for the purpose of modifying, amending, or terminating the plan. The rule provides that summary information is information that summarizes claims history, claims expenses, or types of claims experienced by individuals for whom the plan sponsor has provided health benefits under a group health plan, provided that specified identifiers are not included. Summary information may be disclosed under this provision even if it does not meet the definition of de-identified information. As part of the notice requirements in § 164.520, health plans must inform individuals that they may disclose protected health information to plan sponsors. The provision to allow summaries of claims experience to be disclosed to plan sponsors that purchase insurance will allow them to shop for replacement coverage, and get meaningful bids from prospective issuers. It also permits a plan sponsor to get summary information as part of its consideration of whether or not to change the benefits that are offered or employees or whether or not to terminate a group health plan.

We note that a plan sponsor may perform enrollment functions on behalf of its employees without meeting the conditions above and without using the standard transactions described in the Transactions Rule.

Section 164.504(g)—Multiple Covered Function Entities

Although not addressed in the proposed rule, this final rule also recognizes that a covered entity may as a single legal entity, affiliated entity, or other arrangement combine the functions or operations of health care providers, health plans and health care clearinghouses (for example, integrated health plans and health care delivery systems may function as both health plans and health care providers). The rule permits such covered entities to use or disclose the protected health information of its patients or members for all covered entity functions, consistent with the other requirements of this rule. The health care component must meet the requirements of this rule that apply to a particular type of covered entity when it is functioning as that entity; *e.g.,* when a health care component is operating as a health care provider it must meet the requirements of this rule applicable to a health care provider. However, such covered entities may not use or disclose the protected health information of an individual who is not involved in a particular covered entity function for that function, and such information must be segregated from any joint information systems. For example, an HMO may integrate data about health plan members and clinic services to members, but a health care system may not share information about a patient in its hospital with its health plan if the patient is not a member of the health plan.

Section 164.506—Uses and Disclosures for Treatment, Payment, and Health Care Operations

Introduction: ''Consent'' versus ''Authorization''

In the proposed rule, we used the term ''authorization'' to describe the individual's written permission for a covered entity to use and disclose protected health information, regardless of the purpose of the use or disclosure. Authorization would have been required for all uses and disclosures that were not otherwise permitted or required under the NPRM.

We proposed to permit covered entities, subject to limited exceptions for psychotherapy notes and research information unrelated to treatment, to use and disclose protected health information to carry out treatment, payment, and health care operations without authorization. See proposed § 164.506(a)(1).

We also proposed to prohibit covered entities from requiring individuals to sign authorizations for uses and disclosures of protected health information for treatment, payment, and health care operations, unless required by other applicable law. See proposed § 164.508(a)(iv). We instead proposed requiring covered entities to produce a notice describing their information practices, including practices with respect to uses and disclosures to carry out treatment, payment, and health care operations.

In the final rule, we retain the requirement for covered entities to obtain the individual's written permission (an ''authorization'') for uses and disclosures of protected health information that are not otherwise permitted or required under the rule. However, under the final rule, we add a second type of written permission for use or disclosure of protected health information: a ''consent'' for uses and disclosures to carry out treatment, payment, and health care operations. In the final rule, we permit, and in some cases require, covered entities to obtain the individual's written permission for the covered entity to use or disclose protected health information other than psychotherapy notes to carry out treatment, payment, and health care operations. We refer to this written permission as a ''consent.''

The ''consent'' and the ''authorization'' do not overlap. The requirement to obtain a ''consent'' applies in different circumstances than the requirement to obtain an authorization. In content, a consent and an authorization differ substantially from one another.

As described in detail below, a ''consent'' allows use and disclosure of protected health information only for treatment, payment, and health care operations. It is written in general terms and refers the individual to the covered entity's notice for further information about the covered entity's privacy practices. It allows use and disclosure of protected health information by the covered entity seeking the consent, not by other persons. Most persons who obtain a consent will be health care providers; health plans and health care clearinghouses may also seek a consent. The consent requirements appear in § 164.506 and are described in this section of the preamble.

With a few exceptions, an ''authorization'' allows use and disclosure of protected health information for purposes other than treatment, payment, and health care

operations. In order to make uses and disclosures that are not covered by the consent requirements and not otherwise permitted or required under the final rule, covered entities must obtain the individual's ''authorization.'' An ''authorization'' must be written in specific terms. It may allow use and disclosure of protected health information by the covered entity seeking the authorization, or by a third party. In some instances, a covered entity may not refuse to treat or cover individuals based on the fact that they refuse to sign an authorization. See § 164.508 and the corresponding preamble discussion regarding authorization requirements.

Section 164.506(a)—Consent Requirements

We make significant changes in the final rule with respect to uses and disclosures of protected health information to carry out treatment, payment, and health care operations. We do not prohibit covered entities from seeking an individual's written permission for use or disclosure of protected health information to carry out treatment, payment, or health care operations.

Except as described below, we instead require covered health care providers to obtain the individual's consent prior to using or disclosing protected health information to carry out treatment, payment, or health care operations. If the covered provider does not obtain the individual's consent, the provider is prohibited from using or disclosing protected health information about the individual for purposes of treating the individual, obtaining payment for health care delivered to the individual, or for the provider's health care operations. See § 164.506(a)(1).

We except two types of health care providers from this consent requirement. First, covered health care providers that have an indirect treatment relationship with an individual are not required to obtain the individual's consent prior to using or disclosing protected health information about the individual to carry out treatment, payment, and health care operations. An ''indirect treatment relationship'' is defined in § 164.501 and described in the corresponding preamble. These providers may use and disclose protected health information as otherwise permitted under the rule and consistent with their notice of privacy practices (see § 164.520 regarding notice requirements and § 164.502(i) regarding requirements to adhere to the notice). For example, a covered provider that provides consultation services to another provider without seeing the patient would have an indirect treatment relationship with that patient and would not be required to obtain the patient's consent to use protected health information about the patient for the consultation. These covered providers are, however, permitted to obtain consent, as described below.

Second, covered health care providers that create or receive protected health information in the course of providing health care to inmates of a correctional institution are not required to obtain the inmate's consent prior to using or disclosing protected health information about the inmate to carry out treatment, payment, and health care operations. See § 164.501 and the corresponding preamble discussion regarding the definitions of ''correctional institution'' and ''inmate.'' These providers may use and disclose protected health information as otherwise permitted under the rule. These providers are permitted, however, to obtain consent, as described below.

In addition, we permit covered health care providers to use and disclose protected health information, without consent, to carry out treatment, payment, and health care operations, if the protected health information was created or received in certain treatment situations. In the treatment situations described in § 164.506(a)(3) and immediately below, the covered health care provider must attempt to obtain the individual's consent. If the covered provider is unable to obtain consent, but documents the attempt and the reason consent was not obtained, the covered provider may, without consent, use and disclose the protected health information resulting from the treatment as otherwise permitted under the rule. All other protected health information about that individual that the covered health care provider creates or receives, however, is subject to the consent requirements.

This exception to the consent requirement applies to protected health information created or received in any of three treatment situations. First, the exception applies to protected health information created or received in emergency treatment situations. In these situations, covered providers must attempt to obtain the consent as soon as reasonably practicable after the delivery of the emergency treatment. Second, the exception applies to protected health information created or received in situations where the covered health care provider is required by law to treat the individual (for example, certain publicly funded providers) and the covered health care provider attempts to obtain such consent. Third, the exception applies to protected health information created or received in treatment situations where there are substantial barriers to communicating with the individual and, in the exercise of professional judgment, the covered provider clearly infers from the circumstances the individual's consent to receive treatment. For example, there may be situations in which a mentally incapacitated individual seeks treatment from a health care provider but is unable to provide informed consent to undergo such treatment and does not have a personal representative available to provide such consent on the individual's behalf. If the covered provider, in her professional judgment, believes she can legally provide treatment to that individual, we also permit the provider to use and disclose protected health information resulting from the treatment without the individual's consent. We intend covered health care providers that legally provide treatment without the individual's consent to that treatment to be able to use and disclose protected health information resulting from that treatment to carry out treatment, payment, or health care operations without obtaining the individual's consent for such use or disclosure. We do not intend to impose unreasonable barriers to individuals' ability to receive, and health care providers' ability to provide, health care.

Under § 164.506(a)(4), covered health care providers that have an indirect treatment relationship with an individual, as well as health plans and health care clearinghouses, may elect to seek consent for their own uses and disclosures to carry out treatment, payment, and health care operations. If such a covered entity seeks consent for these purposes, the consent must meet the minimum requirements described below.

If a covered health care provider with an indirect treatment relationship, a health plan, or a health care clearinghouse does not seek consent, the covered entity may use or disclose protected health information to carry out treatment, payment, and health care operations as otherwise permitted under the rule and consistent with its notice of privacy practices (see § 164.520 regarding notice requirements and § 164.502(i) regarding requirements to adhere to the notice).

If a covered health care provider with an indirect treatment relationship, a health plan, or a health care clearinghouse does ask an individual to sign a consent, and the individual does not do so, the covered entity is

prohibited under § 164.502(a)(1) from using or disclosing protected health information for the purpose(s) included in the consent. A covered entity that seeks a consent must adhere to the individual's decision.

In § 164.506(a)(5), we specify that a consent obtained by one covered entity is not effective to permit another covered entity to use or disclose protected health information, unless the consent is a joint consent. See § 164.506(f) and the corresponding preamble discussion below regarding joint consents. A consent provides the individual's permission only for the covered entity that obtains the consent to use or disclose protected health information for treatment, payment, and health care operations. A consent under this section does not operate to authorize another covered entity to use or disclose protected health information, except where the other covered entity is operating as a business associate. We note that, where a covered entity is acting as a business associate of another covered entity, the business associate covered entity is acting for or on behalf of the principal covered entity, and its actions for or on behalf of the principal covered entity are authorized by the consent obtained by the principal covered entity. Thus, under this section, a health plan can obtain a consent that permits the health plan and its business associates to use and disclose protected health information that the health plan and its business associates create or receive. That consent cannot, however, permit another covered entity (that is not a business associate) to disclose protected health information to the health plan or to any other person.

If a covered entity wants to obtain the individual's permission for another covered entity to disclose protected health information to it for treatment, payment, or health care operations purposes, it must seek an authorization in accordance with § 164.508(e). For example, when a covered provider asks the individual for written permission to obtain the individual's medical record from another provider for treatment purposes, it must do so with an authorization, not a consent. Since the permission is for disclosure of protected health information by another person, a consent may not be used.

Section 164.506(b)—Consent General Requirements

In the final rule, we permit a covered health care provider to condition the provision of treatment on the receipt of the individual's consent for the covered provider to use and disclose protected health information to carry out treatment, payment, and health care operations. Covered providers may refuse to treat individuals who do not consent to uses and disclosures for these purposes. See § 164.506(b)(1). We note that there are exceptions to the consent requirements for covered health care providers that are required by law to treat individuals. See § 164.506(a)(3), described above.

Similarly, in the final rule, we permit health plans to condition an individual's enrollment in the health plan on the receipt of the individual's consent for the health plan to use and disclose protected health information to carry out treatment, payment, and health care operations, if the consent is sought in conjunction with the enrollment process. If the health plan seeks the individual's consent outside of the enrollment process, the health plan may not condition any services on obtaining such consent.

Under § 164.520, covered entities must produce a notice of privacy practices. A consent may not be combined in a single document with the notice of privacy practices. See § 164.506(b)(3).

Under § 164.506(b)(4), consents for uses and disclosures of protected health information to carry out treatment, payment, and health care operations may be combined in a single document covering all three types of activities and may be combined with other types of legal permission from the individual. For example, a consent to use or disclose protected health information under this rule may be combined with an informed consent to receive treatment, a consent to assign payment of benefits to a provider, or narrowly tailored consents required under state law for the use or disclosure of specific types of protected health information (*e.g.,* state laws requiring specific consent for any sharing of information related to HIV/AIDS).

Within a single consent document, the consent for use and disclosure of protected health information required or permitted under this rule must be visually and organizationally separate from the other consents or authorizations and must be separately signed by the individual and dated.

Where research includes treatment of the individual, a consent under this rule may be combined with the authorization for the use or disclosure of protected health information created for the research, in accordance with § 164.508(f). (This is the only case in which an authorization under § 164.508 of this rule may be combined with a consent under § 164.506 of this rule. See § 164.508(b)(3).) The covered entity that is creating protected health information for the research may elect to combine the consent required under this section with the research-related authorization required under § 164.508(f). For example, a covered health care provider that provides health care to an individual for research purposes and for non-research purposes must obtain a consent under this section for all of the protected health information it maintains. In addition, it must obtain an authorization in accordance with § 164.508(f) which describes how it will use and disclose the protected health information it creates for the research for purposes of treatment, payment, and health care operations. Section 164.506(b)(4) permits the covered entity to satisfy these two requirements with a single document. See § 164.508(f) and the corresponding preamble discussion for a more detailed description of research authorization requirements.

Under § 164.506(b)(5), individuals may revoke a consent in writing at any time, except to the extent that the covered entity has taken action in reliance on the consent. Upon receipt of the written revocation, the covered entity must stop processing the information for use or disclosure, except to the extent that it has taken action in reliance on the consent. A covered health care provider may refuse, under this rule, to continue to treat an individual that revokes his or her consent. A health plan may disenroll an individual that revokes a consent that was sought in conjunction with the individual's enrollment in the health plan.

Covered entities must document and retain any signed consent as required by § 164.530(j).

Section 164.506(c)—Consent Content Requirements

Under § 164.506(c), the consent must be written in plain language. See the preamble discussion regarding notice of privacy practices for a description of plain language requirements. We do not provide a model consent in this rule. We will provide further guidance on drafting consent documents prior to the compliance date.

Under § 164.506(c)(1), the consent must inform the individual that protected health information may be used and disclosed by the covered entity to carry out treatment, payment, or health care operations. The covered entity must determine which of these elements (use and/or disclosure; treatment, payment, and/or health care operations) to include in the consent

document, as appropriate for the covered entity's practices.

For covered health care providers that are required to obtain consent, the requirement applies only to the extent the covered provider uses or discloses protected health information. For example, if all of a covered provider's health care operations are conducted by members of the covered provider's own workforce, the covered provider may choose to obtain consent only for uses, not disclosures, of protected health information to carry out health care operations. If an individual pays out of pocket for all services received from the covered provider and the provider will not disclose any information about the patient to a third party payor, the provider may choose not to obtain the individual's consent to disclose information for payment purposes. In order for a covered provider to be able to use and disclose information for all three purposes, however, all three purposes must be included in the consent.

Under §§ 164.506(c)(2) and (3), the consent must refer the individual to the covered entity's notice for additional information about the uses and disclosures of information described in the consent. The consent must also indicate that the individual has the right to review the notice prior to signing the consent. If the covered entity has reserved the right to change its privacy practices in accordance with § 164.520(b)(1)(v)(C), the consent must indicate that the terms of the notice may change and must describe how the individual may obtain a revised notice. See § 164.520 and the corresponding preamble discussion regarding notice requirements.

Under § 164.506(c)(4), the consent must inform individuals that they have the right to request restrictions on uses and disclosures of protected health information for treatment, payment, and health care operations purposes. It must also state that the covered entity is not required to agree to an individual's request, but that if the covered entity does agree to the request, the restriction is binding on the covered entity. See § 164.522(a) regarding the right to request restrictions.

Under § 164.506(c)(5), the consent must indicate that the individual has the right to revoke the consent in writing, except to the extent that the covered entity has taken action in reliance on the consent.

Under § 164.506(c)(6), the consent must include the individual's signature and the date of signature. Once we adopt the standards for electronic signature, another of the required administrative simplification standards we are required to adopt under HIPAA, an electronic signature that meets those standards will be sufficient under this rule. We do not require any verification of the individual's identity or authentication of the individual's signature. We expect covered health care providers that are required to obtain consent to employ the same level of scrutiny to these signatures as they do to the signature obtained on a document regarding the individual's consent to undergo treatment by the provider.

Section 164.506(d)—Defective Consents

Under § 164.506(d), there is no ''consent'' within the meaning of the rule if the completed document lacks a required element or if the individual has revoked the consent in accordance with § 164.506(b)(5).

Section 164.506(e)—Resolving Conflicting Consents and Authorizations

Situations may arise where a covered entity that has obtained the individual's consent for the covered entity to use or disclose protected health information to carry out treatment, payment, or health care operations is asked to disclose protected health information pursuant to another written legal permission from the individual, such as an authorization, that was obtained by another person. Under § 164.506(e), when the terms of a covered entity's consent conflict with the terms of another written legal permission from the individual to use or disclose protected health information (such as a consent obtained under state law by another covered entity or an authorization), the covered entity must adhere to the more restrictive document. By conflict, we mean that the consent and authorization contain inconsistencies. In implementing this section, we note that the consent under this section references the notice provided to the individual and the individual's right to request restrictions. In determining whether the covered entity's consent conflicts with another written legal permission provided by the individual, the covered entity must consider any limitations on its uses or disclosures resulting from the notice provided to the individual or from restrictions to which it has agreed. For example, a covered nursing home may elect to ask the patient to sign an authorization for the patient's covered primary care physician to forward the patient's medical records to the nursing home. The physician may have previously obtained the individual's consent for disclosure for treatment purposes. If the authorization obtained by the nursing home grants permission for the physician to disclose particular types of information, such as genetic information, but the consent obtained by the physician excludes such information or the physician has agreed to a restriction on that type of information, the physician may not disclose that information. The physician must adhere to the more restrictive written legal permission from the individual.

When a conflict between a consent and another written legal permission from the individual exists, as described above, the covered entity may attempt to resolve the conflict with the individual by either obtaining a new consent from the individual or by having a discussion or otherwise communicating with the individual to determine the individual's preference regarding the use or disclosure. If the individual's preference is communicated orally, the covered entity must document the individual's preference and act in accordance with that preference. In the example described above, the primary care physician could ask the patient to sign a new consent that would permit the disclosure of the genetic information. Alternatively, the physician could ask the patient whether the patient intended for the genetic information to be disclosed to the nursing home. If the patient confirms that he or she intended for the genetic information to be shared, the physician can document that fact (*e.g.,* by making a notation in the medical record) and disclose the information to the nursing home.

We believe covered entities will rarely be faced with conflicts between consents and other written legal permission from the individual for uses and disclosures to carry out treatment, payment, and health care operations. Under § 164.506(a)(5), we specify that a consent only permits the covered entity that obtains the consent to use or disclose protected health information. A consent obtained by one covered entity is not effective to permit another different covered entity to use or disclose protected health information. Conflicting consents obtained by covered entities, therefore, are not possible. We expect authorizations that permit another covered entity to use and disclose protected health information for treatment, payment, and health care operations purposes will rarely be necessary, because we expect covered entities that maintain protected health information to obtain consents that permit them to make anticipated uses and disclosures for these purposes. Nevertheless, covered entities are permitted under § 164.508(e) to obtain

authorization for another covered entity to use or disclose protected health information to carry out treatment, payment, and health care operations. We recognize these authorizations may be useful to demonstrate an individual's intent and relationship to the intended recipient of the information. For example, these authorizations may be useful in situations where a health plan wants to obtain information from one provider in order to determine payment of a claim for services provided by a different provider (e.g., information from a primary care physician that is necessary to determine payment of services provided by a specialist) or where an individual's new physician wants to obtain the individual's medical records from prior physicians. Other persons not covered by this rule may also seek authorizations and state law may require written permission for specific types of information, such as information related to HIV/AIDS or to mental health. Because an individual may sign conflicting documents over time, we clarify that the covered entity maintaining the protected health information to be used or disclosed must adhere to the more restrictive permission the individual has granted, unless the covered entity resolves the conflict with the individual.

Section 164.506(f)—Joint Consents

Covered entities that participate in an organized health care arrangement and that develop a joint notice under § 164.520(d) may develop a joint consent in which the individual consents to the uses and disclosures of protected health information by each of the covered entities in the arrangement to carry out treatment, payment, and/or health care operations. The joint consent must identify with reasonable specificity the covered entities, or class of covered entities, to which the joint consent applies and must otherwise meet the consent requirements. If an individual revokes a joint consent, the covered entity that receives the revocation must inform the other entities covered by the joint consent of the revocation as soon as practicable.

If any one of the covered entities included in the joint consent obtains the individual's consent, as required above, the consent requirement is met for all of the other covered entities to which the consent applies. For example, a covered hospital and the clinical laboratory and emergency departments with which it participates in an organized health care arrangement may produce a joint notice and obtain a joint consent. If the covered hospital obtains the individual's joint consent upon admission, and some time later the individual is readmitted through the associated emergency department, the emergency department's consent requirement will already have been met. These joint consents are the only type of consent by which one covered entity can obtain the individual's permission for another covered entity to use or disclose protected health information to carry out treatment, payment, or health care operations.

Effect of Consent

These consents, as well as the authorizations described in § 164.508, should not be construed to waive, directly or indirectly, any privilege granted under federal, state, or local law or procedure. Consents obtained under this regulation are not appropriate for the disposition of more technical and legal proceedings and may not comport with procedures and standards of federal, state, or local judicial practice. For example, state courts and other decision-making bodies may choose to examine more closely the circumstances and propriety of such consent and may adopt more protective standards for application in their proceedings. In the judicial setting, as in the legislative and executive settings, states may provide for greater protection of privacy. Additionally, both the Congress and the Secretary have established a general approach to protecting from explicit preemption state laws that are more protective of privacy than the protections set forth in this regulation.

Section 164.508—Uses and Disclosures for Which an Authorization Is Required

Section 164.508(a)—Standard

We proposed to require covered entities to obtain the individual's authorization for all uses and disclosures of protected health information not otherwise permitted or required under the proposed rule. Uses and disclosures that would have been permitted without individual authorization included uses and disclosures for national priority purposes such as public health, law enforcement, and research (see proposed § 164.510) and uses and disclosures of protected health information, other than psychotherapy notes and research information unrelated to treatment, for purposes of treatment, payment, and health care operations (see proposed § 164.506). We also proposed to require covered entities to disclose protected health information to the individual for inspection and copying (see proposed § 164.514) and to the Secretary as required for enforcement of the rule (see proposed § 164.522). Individual authorization would not have been required for these uses and disclosures.

We proposed to require covered entities to obtain the individual's authorization for all other uses and disclosures of protected health information. Under proposed § 164.508(a), uses and disclosures that would have required individual authorization included, but were not limited to, the following:

- Use for marketing of health and non-health items and services by the covered entity;
- Disclosure by sale, rental, or barter;
- Use and disclosure to non-health related divisions of the covered entity, e.g., for use in marketing life or casualty insurance or banking services;
- Disclosure, prior to an individual's enrollment in a health plan, to the health plan or health care provider for making eligibility or enrollment determinations relating to the individual or for underwriting or risk rating determinations;
- Disclosure to an employer for use in employment determinations; and
- Use or disclosure for fundraising.

In the preamble to the proposed rule, we stated that covered entities would be bound by the terms of authorizations. Uses or disclosures by the covered entity for purposes inconsistent with the statements made in the authorization would have constituted a violation of the rule.

In the final rule, under § 164.508(a), as in the proposed rule, covered entities must have authorization from individuals before using or disclosing protected health information for any purpose not otherwise permitted or required by this rule. Specifically, except for psychotherapy notes (see below), covered entities are not required to obtain the individual's authorization to use or disclose protected health information to carry out treatment, payment, and health care operations. (Covered entities may, however, be required to obtain the individual's consent for these uses and disclosures. See the preamble regarding § 164.506 for a discussion of ''consent'' versus ''authorization''.) We also do not require covered entities to obtain the individual's authorization for uses and disclosures of protected health information permitted under §§ 164.510 or 164.512, for disclosures to the individual, or for required disclosures to the Secretary under subpart C of part 160 of this subchapter for enforcement of this rule.

In the final rule, we clarify that covered entities are bound by the

statements provided on the authorization; use or disclosure by the covered entity for purposes inconsistent with the statements made in the authorization constitutes a violation of this rule.

Unlike the proposed rule, we do not include in the regulation examples of the types of uses and disclosures that require individual authorization. We eliminated two examples from the proposed list due to potential confusion as to our intent: disclosure by sale, rental, or barter and use and disclosure to non-health related divisions of the covered entity. We recognize that covered entities sometimes make these types of uses and disclosures for purposes that are permitted under the rule without authorization. For example, a covered health care provider may sell its accounts receivable to a collection agency for payment purposes and a health plan may disclose protected health information to its life insurance component for payment purposes. We do not intend to require authorization for uses and disclosures made by sale, rental, or barter or for disclosures made to non-health related divisions of the covered entity, if those uses or disclosures could otherwise be made without authorization under this rule. As with any other use or disclosure, however, uses and disclosures of protected health information for these purposes do require authorization if they are not otherwise permitted under the rule.

We also eliminated the remaining proposed examples from the final rule due to concern that these examples might be misinterpreted as an exhaustive list of all of the uses and disclosures that require individual authorization. We discuss the examples here, however, to clarify the interaction of the authorization requirements and the provisions of the rule that permit uses and disclosures without authorization and/or with consent. Uses and disclosures for which covered entities must have the individual's authorization include, but are not limited to, the following activities.

Marketing

As in the proposed rule, covered entities must obtain the individual's authorization before using or disclosing protected health information for marketing purposes. In the final rule, we add a new definition of marketing (see § 164.501). For more detail on what activities constitute marketing, see § 164.501, definition of ''marketing,'' and § 164.514(e).

Pre-Enrollment Underwriting

As in the proposed rule, covered entities must obtain the individual's authorization to use or disclose protected health information for the purpose of making eligibility or enrollment determinations relating to an individual or for underwriting or risk rating determinations, prior to the individual's enrollment in a health plan (that is, for purposes of pre-enrollment underwriting). For example, if an individual applies for new coverage with a health plan in the non-group market and the health plan wants to review protected health information from the individual's covered health care providers before extending an offer of coverage, the individual first must authorize the covered providers to share the information with the health plan. If the individual applies for renewal of existing coverage, however, the health plan would not need to obtain an authorization to review its existing claims records about that individual, because this activity would come within the definition of health care operations and be permissible. We also note that under § 164.504(f), a group health plan and a health insurance issuer that provides benefits with respect to a group health plan are permitted in certain circumstances to disclose summary health information to the plan sponsor for the purpose of obtaining premium bids. Because these disclosures fall within the definition of health care operations, they do not require authorization.

Employment Determinations

As in the proposed rule, covered entities must obtain the individual's authorization to use or disclose protected health information for employment determinations. For example, a covered health care provider must obtain the individual's authorization to disclose the results of a pre-employment physical to the individual's employer. The final rule provides that a covered entity may condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party on the provision of authorization for the disclosure of the information to the third party.

Fundraising

Under the proposed regulation, we would have required authorization before a covered entity could have used or disclosed protected health information for fundraising. In the final rule, we narrow the circumstances under which covered entities must obtain the individual's authorization to use or disclose protected health information for fundraising purposes. As provided in § 164.514(f) and described in detail in the corresponding preamble, authorization is not required when a covered entity uses or discloses demographic information and information about the dates of health care provided to an individual for the purpose of raising funds for its own benefit, nor when it discloses such information to an institutionally related foundation to raise funds for the covered entity.

Any use or disclosure for fundraising purposes that does not meet the requirements of § 164.514(f) and does not fall within the definition of health care operations (see § 164.501), requires authorization. Specifically, covered entities must obtain the individual's authorization to use or disclose protected health information to raise funds for any entity other than the covered entity. For example, a covered entity must have the individual's authorization to use protected health information about the individual to solicit funds for a non-profit organization that engages in research, education, and awareness efforts about a particular disease.

Psychotherapy Notes

In the NPRM, we proposed different rules with respect to psychotherapy notes than we proposed with respect to all other protected health information. The proposed rule would have required covered entities to obtain an authorization for any use or disclosure of psychotherapy notes to carry out treatment, payment, or health care operations, unless the use was by the person who created the psychotherapy notes. With respect to all other protected health information, we proposed to prohibit covered entities from requiring authorization for uses and disclosures for these purposes.

We significantly revise our approach to psychotherapy notes in the final rule. With a few exceptions, covered entities must obtain the individual's authorization to use or disclose psychotherapy notes to carry out treatment, payment, or health care operations. A covered entity must obtain the individual's consent, but not an authorization, for the person who created the psychotherapy notes to use the notes to carry out treatment and for the covered entity to use or disclose psychotherapy notes for conducting training programs in which students, trainees, or practitioners in mental health learn under supervision to

practice or improve their skills in group, joint, family, or individual counseling. A covered entity may also use psychotherapy notes to defend a legal action or other proceeding brought by the individual pursuant to a consent, without a specific authorization. We note that, while this provision allows disclosure of these records to the covered entity's attorney to defend against the action or proceeding, disclosure to others in the course of a judicial or administrative proceeding is governed by § 164.512(e). This special provision is necessary because disclosure of protected health information for purposes of legal representatives may be made under the general consent as part of ''health care operations.'' Because we require an authorization for disclosure of psychotherapy notes for ''health care operations,'' an exception is needed to allow covered entities to use protected health information about an individual to defend themselves against an action threatened or brought by that individual without asking that individual for authorization to do so. Otherwise, a consent under § 164.506 is not sufficient for the use or disclosure of psychotherapy notes to carry out treatment, payment, or health care operations. Authorization is required. We anticipate these authorizations will rarely be necessary, since psychotherapy notes do not include information that covered entities typically need for treatment, payment, or other types of health care operations.

In the NPRM, we proposed to permit covered entities to use and disclose psychotherapy notes for all other purposes permitted or required under the rule without authorization. In the final rule, we specify a more limited set of uses and disclosures of psychotherapy notes that covered entities are permitted to make without authorization. An authorization is not required for use or disclosure of psychotherapy notes when required for enforcement purposes, in accordance with subpart C of part 160 of this subchapter; when mandated by law, in accordance with § 164.512(a); when needed for oversight of the health care provider who created the psychotherapy notes, in accordance with § 164.512(d); when needed by a coroner or medical examiner, in accordance with § 164.512(g)(1); or when needed to avert a serious and imminent threat to health or safety, in accordance with § 164.512(j)(1)(i). We also provide transition provisions in § 164.532 regarding the effect of express legal permission obtained from an individual prior to the compliance date of this rule.

Section 164.508(b)—Implementation Specifications for Authorizations

Valid and Defective Authorizations

We proposed to require a minimum set of elements for authorizations requested by the individual and an additional set of elements for authorizations requested by a covered entity. We would have permitted covered entities to use and disclose protected health information pursuant to authorizations containing the applicable required elements. We would have prohibited covered entities from acting on an authorization if the submitted document had any of the following defects:

- The expiration date had passed;
- The form had not been filled out completely;
- The covered entity knew the authorization had been revoked;
- The completed form lacked a required element; or
- The covered entity knew the information on the form was false.

In § 164.508(b)(1) of the final rule, we specify that an authorization containing the applicable required elements (as described below) is a valid authorization. We clarify that a valid authorization may contain additional, non-required elements, provided that these elements are not inconsistent with the required elements. Covered entities are not required to use or disclose protected health information pursuant to a valid authorization. Our intent is to clarify that a covered entity that uses or discloses protected health information pursuant to an authorization meeting the applicable requirements will be in compliance with this rule.

We retain the provision prohibiting covered entities from acting on an authorization if the submitted document had any of the listed defects, with a few changes. First, in § 164.508(c)(1)(iv) we specify that an authorization may expire upon a certain event or on a specific date. For example, a valid authorization may state that it expires upon acceptance or rejection of an application for insurance or upon the termination of employment (for example, in an authorization for disclosure of protected health information for fitness-for-duty purposes) or similar event. The expiration event must, however, be related to the individual or the purpose of the use or disclosure. An authorization that purported to expire on the date when the stock market reached a specified level would not be valid. Under § 164.508(b)(2)(i), if the expiration event is known by the covered entity to have occurred, the authorization is defective. Second, we clarify that certain compound authorizations, as described below, are defective. We also clarify that authorizations that are not completely filled out with respect to the required elements are defective. Finally, we clarify that an authorization with information that the covered entity knows to be false is defective only if the information is material.

As under the proposed regulation, an authorization that the covered entity knows has been revoked is not a valid authorization. We note that, although an authorization must be revoked in writing, the covered entity may not always ''know'' that an authorization has been revoked. The writing required for an individual to revoke an authorization may not always trigger the ''knowledge'' required for a covered entity to consider an authorization defective. Conversely, a copy of the written revocation is not required before a provider ''knows'' that an authorization has been revoked.

Many authorizations will be obtained by persons other than the covered entity. If the individual revokes an authorization by writing to that other person, and neither the individual nor the other person informs the covered entity of the revocation, the covered entity will not ''know'' that the authorization has been revoked. For example, a government agency may obtain an individual's authorization for ''all providers who have seen the individual in the past year'' to disclose protected health information to the agency for purposes of determining eligibility for benefits. The individual may revoke the authorization by writing to the government agency requesting such revocation. We cannot require the agency to inform all covered entities to whom it has presented the authorization that the authorization has been revoked. If a covered entity does not know of the revocation, the covered entity will not violate this rule by acting pursuant to the authorization. At the same time, if the individual does inform the covered entity of the revocation, even orally, the covered entity ''knows'' that the authorization has been revoked and can no longer treat the authorization as valid under this rule. Thus, in this example, if the individual tells a covered entity that the individual has revoked the authorization, the covered entity ''knows'' of the revocation and must consider the authorization defective under § 164.508(b)(2).

Compound Authorizations

Except for authorizations requested in connection with a clinical trial, we proposed to prohibit covered entities from combining an authorization for use or disclosure of protected health information for purposes other than treatment, payment, or health care operations with an authorization or consent for treatment (*e.g.,* an informed consent to receive care) or payment (*e.g.,* an assignment of benefits).

We clarify the prohibition on compound authorizations in the final rule. Other than as described below, § 164.508(b)(3) prohibits a covered entity from acting on an authorization required under this rule that is combined with any other document, including any other written legal permission from the individual. For example, an authorization under this rule may not be combined with a consent for use or disclosure of protected health information under § 164.506, with the notice of privacy practices under § 164.520, with any other form of written legal permission for the use or disclosure of protected health information, with an informed consent to participate in research, or with any other form of consent or authorization for treatment or payment.

There are three exceptions to this prohibition. First, under § 164.508(f) (described in more detail, below), an authorization for the use or disclosure of protected health information created for research that includes treatment of the individual may be combined with a consent for the use or disclosure of that protected health information to carry out treatment, payment, or health care operations under § 164.506 and with other documents as provided in § 164.508(f). Second, authorizations for the use or disclosure of psychotherapy notes for multiple purposes may be combined in a single document, but may not be combined with authorizations for the use or disclosure of other protected health information. Third, authorizations for the use or disclosure of protected health information other than psychotherapy notes may be combined, provided that the covered entity has not conditioned the provision of treatment, payment, enrollment, or eligibility on obtaining the authorization. If a covered entity conditions any of these services on obtaining an authorization from the individual, as permitted in § 164.508(b)(4) and described below, the covered entity must not combine the authorization with any other document.

The following are examples of valid compound authorizations: an authorization for the disclosure of information created for clinical research combined with a consent for the use or disclosure of other protected health information to carry out treatment, payment, and health care operations, and the informed consent to participate in the clinical research; an authorization for disclosure of psychotherapy notes for both treatment and research purposes; and an authorization for the disclosure of the individual's demographic information for both marketing and fundraising purposes. Examples of invalid compound authorizations include: an authorization for the disclosure of protected health information for treatment, for research, and for determining payment of a claim for benefits, when the covered entity will refuse to pay the claim if the individual does not sign the authorization; or an authorization for the disclosure of psychotherapy notes combined with an authorization to disclose any other protected health information.

Prohibition on Conditioning Treatment, Payment, Eligibility, or Enrollment

We proposed to prohibit covered entities from conditioning treatment or payment on the provision by the individual of an authorization, except when the authorization was requested in connection with a clinical trial. In the case of authorization for use or disclosure of psychotherapy notes or research information unrelated to treatment, we proposed to prohibit covered entities from conditioning treatment, payment, or enrollment in a health plan on obtaining such an authorization.

We retain this basic approach but refine its application in the final rule. In addition to the general prohibition on conditioning treatment and payment, covered entities are also prohibited (with certain exceptions described below) from conditioning eligibility for benefits or enrollment in a health plan on obtaining an authorization. This prohibition extends to all authorizations, not just authorizations for use or disclosure of psychotherapy notes. This prohibition is intended to prevent covered entities from coercing individuals into signing an authorization for a use or disclosure that is not necessary to carry out the primary services that the covered entity provides to the individual. For example, a health care provider could not refuse to treat an individual because the individual refused to authorize a disclosure to a pharmaceutical manufacturer for the purpose of marketing a new product.

We clarify the proposed research exception to this prohibition. Covered entities seeking authorization in accordance with § 164.508(f) to use or disclose protected health information created for the purpose of research that includes treatment of the individual, including clinical trials, may condition the research-related treatment on the individual's authorization. Permitting use of protected health information is part of the decision to receive care through a clinical trial, and health care providers conducting such trials should be able to condition research-related treatment on the individual's willingness to authorize the use or disclosure of his or her protected health information for research associated with the trial.

In addition, we permit health plans to condition eligibility for benefits and enrollment in the health plan on the individual's authorization for the use or disclosure of protected health information for purposes of eligibility or enrollment determinations relating to the individual or for its underwriting or risk-rating determinations. We also permit health plans to condition payment of a claim for specified benefits on the individual's authorization for the disclosure of information maintained by another covered entity to the health plan, if the disclosure is necessary to determine payment of the claim. These exceptions do not apply, however, to authorization for the use or disclosure of psychotherapy notes. Health plans may not condition payment, eligibility, or enrollment on the receipt of an authorization for the use or disclosure of psychotherapy notes, even if the health plan intends to use the information for underwriting or payment purposes.

Finally, when a covered entity provides treatment for the sole purpose of providing information to a third party, the covered entity may condition the treatment on the receipt of an authorization to use or disclose protected health information related to that treatment. For example, a covered health care provider may have a contract with an employer to provide fitness-for-duty exams to the employer's employees. The provider may refuse to conduct the exam if an individual refuses to authorize the provider to disclose the results of the exam to the employer. Similarly, a covered health care provider may have a contract with a life insurer to provide pre-enrollment physicals to applicants for life insurance coverage. The provider may refuse to conduct the physical if an individual refuses to authorize the provider to disclose the results of the physical to the life insurer.

Revocation of Authorizations

We proposed to allow individuals to revoke an authorization at any time, except to the extent that the covered entity had taken action in reliance on the authorization.

We retain this provision, but specify that the individual must revoke the authorization in writing. When an individual revokes an authorization, a covered entity that knows of such revocation must stop making uses and disclosures pursuant to the authorization to the greatest extent practical. A covered entity may continue to use and disclose protected health information in accordance with the authorization only to the extent the covered entity has taken action in reliance on the authorization. For example, a covered entity is not required to retrieve information that it has already disclosed in accordance with the authorization. (See above for discussion of how written revocation of an authorization and knowledge of that revocation may differ.)

We also include an additional exception. Under § 164.508(b)(5), individuals do not have the right to revoke an authorization if the authorization was obtained as a condition of obtaining insurance coverage and other applicable law provides the insurer that obtained the authorization with the right to contest a claim under the policy. We intend this exception to permit insurers to obtain necessary protected health information during contestability periods under state law. For example, an individual may not revoke an authorization for the disclosure of protected health information to a life insurer for the purpose of investigating material misrepresentation if the individual's policy is still subject to the contestability period.

Documentation

In the final rule, we clarify that a covered entity must document and retain any signed authorization as required by § 164.530(j) (see below).

Section 164.508(c)—Core Elements and Requirements

We proposed to require authorizations requested by individuals to contain a minimum set of elements: a description of the information to be used or disclosed; the name of the covered entity, or class of entities or persons, authorized to make the use or disclosure; the name or types of recipient(s) of the information; an expiration date; the individual's signature and date of signature; if signed by a representative, a description of the representative's authority or relationship to the individual; a statement regarding the individual's right to revoke the authorization; and a statement that the information may no longer be protected by the federal privacy law. We proposed a model authorization form that entities could have used to satisfy the authorization requirements. If the model form was not used, we proposed to require covered entities to use authorization forms written in plain language.

We modify the proposed approach, by eliminating the distinction between authorizations requested by the individuals and authorizations requested by others. Instead, we prescribe a minimum set of elements for authorizations and certain additional elements when the authorization is requested by a covered entity for its own use or disclosure of protected health information it maintains or for receipt of protected health information from another covered entity to carry out treatment, payment, or health care operations.

The core elements are required for all authorizations, not just authorizations requested by individuals. Individuals seek disclosure of protected health information about them to others in many circumstances, such as when applying for life or disability insurance, when government agencies conduct suitability investigations, and in seeking certain job assignments when health status is relevant. Another common instance is tort litigation, when an individual's attorney needs individually identifiable health information to evaluate an injury claim and asks the individual to authorize disclosure of records relating to the injury to the attorney. In each of these situations, the individual may go directly to the covered entity and ask it to send the relevant information to the intended recipient. Alternatively, the intended recipient may ask the individual to complete a form, which the recipient will submit to the covered entity on the individual's behalf, that authorizes the covered entity to disclose the information. Whether the authorization is submitted to the covered entity by the individual or by another person on the individual's behalf, the covered entity maintaining protected health information may not use or disclose it pursuant to an authorization unless the authorization meets the following requirements.

First, the authorization must include a description of the information to be used or disclosed, with sufficient specificity to allow the covered entity to know which information the authorization references. For example, the authorization may include a description of ''laboratory results from July 1998'' or ''all laboratory results'' or ''results of MRI performed in July 1998.'' The covered entity can then use or disclose that information and only that information. If the covered entity does not understand what information is covered by the authorization, the use or disclosure is not permitted unless the covered entity clarifies the request.

There are no limitations on the information that can be authorized for disclosure. If an individual wishes to authorize a covered entity to disclose his or her entire medical record, the authorization can so specify. In order for the covered entity to disclose the entire medical record, the authorization must be specific enough to ensure that the individual has a clear understanding that the entire record will be disclosed. For example, if the Social Security Administration seeks authorization for release of all health information to facilitate the processing of benefit applications, then the description on the authorization form must specify ''all health information'' or the equivalent.

In some instances, a covered entity may be reluctant to undertake the effort to review the record and select portions relevant to the request (or redact portions not relevant). In such circumstances, covered entities may provide the entire record to the individual, who may then redact and release the more limited information to the requestor. This rule does not require a covered entity to disclose information pursuant to an individual's authorization.

Second, the authorization must include the name or other specific identification of the person(s) or class of persons that are authorized to use or disclose the protected health information. If an authorization permits a class of covered entities to disclose information to an authorized person, the class must be stated with sufficient specificity so that a covered entity presented with the authorization will know with reasonable certainty that the individual intended the covered entity to release protected health information. For example, a covered licensed nurse practitioner presented with an authorization for ''all physicians'' to disclose protected health information could not know with reasonable certainty that the individual intended for the practitioner to be included in the authorization.

Third, the authorization must include the name or other specific identification of the person(s) or class of persons to

whom the covered entity is authorized to make the use or disclosure. The authorization must identify these persons with sufficient specificity to reasonably permit a covered entity responding to the authorization to identify the authorized user or recipient of the protected health information. Often, individuals provide authorizations to third parties, who present them to one or more covered entities. For example, an authorization could be completed by an individual and given to a government agency, authorizing the agency to receive medical information from any health care provider that has treated the individual within a defined period of time. Such an authorization is permissible (subject to the other requirements of this part) if it sufficiently identifies the government entity that is authorized to receive the disclosed protected health information.

Fourth, the authorization must state an expiration date or event. This expiration date or event must either be a specific date (*e.g.,* January 1, 2001), a specific time period (*e.g.,* one year from the date of signature), or an event directly relevant to the individual or the purpose of the use or disclosure (*e.g.,* for the duration of the individual's enrollment with the health plan that is authorized to make the use or disclosure). We note that the expiration date or event is subject to otherwise applicable and more stringent law. For example, the National Association of Insurance Commissioners' Insurance Information and Privacy Protection Model Act, adopted in at least fifteen states, specifies that authorizations signed for the purpose of collecting information in connection with an application for a life, health, or disability insurance policy are permitted to remain valid for no longer than thirty months. In those states, the longest such an authorization may remain in effect is therefore thirty months, regardless of the expiration date or event indicated on the form.

Fifth, the authorization must state that the individual has the right to revoke an authorization in writing, except to the extent that action has been taken in reliance on the authorization or, if applicable, during a contestability period. The authorization must include instructions on how the individual may revoke the authorization. For example, the person obtaining the authorization from the individual can include an address where the individual can send a written request for revocation.

Sixth, the authorization must inform the individual that, when the information is used or disclosed pursuant to the authorization, it may be subject to re-disclosure by the recipient and may no longer be protected by this rule.

Seventh, the authorization must include the individual's signature and the date of the signature. Once we adopt the standards for electronic signature, another of the required administrative simplification standards we are required to adopt under HIPAA, an electronic signature that meets those standards will be sufficient under this rule. We do not require verification of the individual's identity or authentication of the individual's signature.

Finally, if the authorization is signed by a personal representative of the individual, the representative must indicate his or her authority to act for the individual.

As in the proposed rule, the authorization must be written in plain language. See the preamble discussion regarding notice of privacy practices (§ 164.520) for a discussion of the plain language requirement. We do not provide a model authorization in this rule. We will provide further guidance on this issue prior to the compliance date.

Section 164.508(d)—Authorizations Requested by a Covered Entity for Its Own Uses and Disclosures

We proposed to require covered entities to include additional elements in authorizations initiated by the covered entity. Before a covered entity could use or disclose protected health information of an individual pursuant to a request the covered entity made, we proposed to require the entity to obtain an authorization containing the minimum elements described above and the following additional elements: except for authorizations requested for clinical trials, a statement that the entity will not condition treatment or payment on the individual's authorization; a description of the purpose of the requested use or disclosure; a statement that the individual may inspect or copy the information to be used or disclosed and may refuse to sign the authorization; and, if the use or disclosure of the requested information will result in financial gain to the entity, a statement that such gain will result.

We additionally proposed to require covered entities, when requesting an individual's authorization, to request only the minimum amount of information necessary to accomplish the purpose for which the request was made. We also proposed to require covered entities to provide the individual with a copy of the executed authorization.

We retain the proposed approach, but apply these additional requirements when the covered entity requests the individual's authorization for the entity's own use or disclosure of protected health information maintained by the covered entity itself. For example, a health plan may ask individuals to authorize the plan to disclose protected health information to a subsidiary to market life insurance to the individual. A pharmaceutical company may also ask a covered provider to recruit patients for drug research; if the covered provider asks patients to sign an authorization for the provider to disclose protected health information to the pharmaceutical company for this research, this is also an authorization requested by a covered entity for disclosure of protected health information maintained by the covered entity. When covered entities initiate the authorization by asking individuals to authorize the entity to use or disclose protected health information that the entity maintains, the authorization must include all of the elements required above as well as several additional elements.

Authorizations requested by covered entities for the covered entity's own use or disclosure of protected health information must state, as applicable under § 164.508(b)(4), that the covered entity will not condition treatment, payment, enrollment, or eligibility on the individual's authorization for the use or disclosure. For example, if a health plan asks an individual to sign an authorization for the health plan to disclose protected health information to a non-profit advocacy group for the advocacy group's fundraising purposes, the authorization must contain a statement that the health plan will not condition treatment, payment, enrollment in the health plan, or eligibility for benefits on the individual providing the authorization.

Authorizations requested by covered entities for their own uses and disclosures of protected health information must also identify each purpose for which the information is to be used or disclosed. The required statement of purpose(s) must provide individuals with the facts they need to make an informed decision whether to allow release of the information. We prohibit the use of broad or blanket authorizations requesting the use or disclosure of protected health information for a wide range of unspecified purposes. Both the information that is to be used or disclosed and the specific purpose(s) for such uses or disclosures must be stated in the authorization.

Authorizations requested by covered entities for their own uses and disclosures must also advise individuals of certain rights available to them under this rule. The authorization must state that the individual may inspect or copy the information to be used or disclosed as provided in § 164.524 regarding access for inspection and copying and that the individual may refuse to sign the authorization.

We alter the proposed requirements with respect to authorizations for which the covered entity will receive financial gain. When the covered entity initiates the authorization and the covered entity will receive direct or indirect remuneration from a third party (rather than financial gain, as proposed) in exchange for using or disclosing the protected health information, the authorization must include a statement that such remuneration will result. For example, a health plan may wish to sell or rent its enrollee mailing list or a pharmaceutical company may offer a covered provider a discount on its products if the provider obtains authorization to disclose the demographic information of patients with certain diagnoses so that the company can market new drugs to them directly. In each case, the covered entity must obtain the individual's authorization, and the authorization must include a statement that the covered entity will receive remuneration.

In § 164.508(d)(2), we continue to require a covered entity that requests an authorization for its own use or disclosure of protected health information to provide the individual with a copy of the signed authorization. While we eliminate from this section the provision requiring covered entities to obtain authorization for use or disclosure of the minimum necessary protected health information, § 164.514(d)(4) requires covered entities to request only the minimum necessary protected health information to accomplish the purpose for which the request is made. This requirement applies to these authorizations, as well as other requests.

Section 164.508(e)—Authorizations Requested by a Covered Entity for Disclosures by Others

In the proposed rule, we would have prohibited all covered entities from requiring the individual's written legal permission (as proposed, an ''authorization'') for the use or disclosure of protected health information to carry out treatment, payment, or health care operations. We generally eliminate this prohibition in the final rule, except to specify that a consent obtained by one covered entity is not effective to permit another covered entity to use or disclose protected health information. See § 164.506(a)(5) and the corresponding preamble discussion.

In the final rule, if a covered entity seeks the individual's written legal permission to obtain protected health information about the individual from another covered entity for any purpose, it must obtain the individual's authorization for the covered entity that maintains the protected health information to make the disclosure. If the authorization is for the purpose of obtaining protected health information for purposes other than treatment, payment, or health care operations, the authorization need only contain the core elements required by § 164.508(c) and described above.

If the authorization, however, is for the purpose of obtaining protected health information to carry out treatment, payment, or health care operations, the authorization must meet the requirements of § 164.508(e). We expect such authorizations will rarely be necessary, because we expect covered entities that maintain protected health information to obtain consents that permit them to make anticipated uses and disclosures for these purposes. An authorization obtained by another covered entity that authorizes the covered entity maintaining the protected health information to make a disclosure for the same purpose, therefore, would be unnecessary.

We recognize, however, that these authorizations may be useful to demonstrate an individual's intent and relationship to the intended recipient of the information when the intent or relationship is not already clear. For example, a long term care insurer may need information from an individual's health care providers about the individual's ability to perform activities of daily living in order to determine payment of a long term care claim. The providers that hold the information may not be providing the long term care and may not, therefore, be aware of the individual's coverage under the policy or that the individual is receiving long term care services. An authorization obtained by the long term care insurer will help to demonstrate these facts to the providers holding the information, which will make them more confident that the individual intends for the information to be shared. Similarly, an insurer with subrogation obligations may need health information from the enrollee's providers to assess or prosecute the claim. A patient's new physician may also need medical records from the patient's prior providers in order to treat the patient. Without an authorization that demonstrates the patient's intent for the information to be shared, the covered entity that maintains the protected health information may be reluctant to provide the information, even if that covered entity's consent permits such disclosure to occur.

These authorizations may also be useful to accomplish clinical coordination and integration among covered entities that do not meet the definitions of affiliated covered entities or organized health care arrangements. For example, safety-net providers that participate in the Community Access Program (CAP) may not qualify as organized health care arrangements but may want to share protected health information with each other in order to develop and expand integrated systems of care for uninsured people. An authorization under this section would permit such providers to receive protected health information from other CAP participants to engage in such activities.

Because of such concerns, we permit a covered entity to request the individual's authorization to obtain protected health information from another covered entity to carry out treatment, payment, and health care operations. In these situations, the authorization must contain the core elements described above and must also describe each purpose of the requested disclosure.

With one exception, the authorization must also indicate that the authorization is voluntary. It must state that the individual may refuse to sign the authorization and that the covered entity requesting the authorization will not condition the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits on obtaining the individual's authorization. If the authorization is for a disclosure of information that is necessary to determine payment of a claim for specified benefits, however, the health plan requesting the authorization may condition the payment of the claim on obtaining the authorization from the individual. See § 164.508(b)(4)(iii). In this case, the authorization does not have to state that the health plan will not condition payment on obtaining the authorization.

The covered entity requesting the authorization must provide the individual with a copy of the signed authorization. We note that the covered entity requesting the authorization is also subject to the requirements in

§ 164.514 to request only the minimum necessary information needed for the purpose of the authorization.

We additionally note that, when the covered entity that maintains the protected health information has already obtained a consent for disclosure of protected health information to carry out treatment, payment, and/or health care operations under § 164.506, and that consent conflicts with an authorization obtained by another covered entity under § 164.508(e), the covered entity maintaining the protected health information is bound by the more restrictive document. See § 164.506(e) and the corresponding preamble discussion for further explanation.

Section 164.508(f)—Authorizations for Uses and Disclosures of Protected Health Information Created for Research that Includes Treatment of Individuals

In the proposed rule, we would have required individual authorization for any use or disclosure of research information unrelated to treatment. In the final rule, we eliminate the special rules for this category of information and, instead, require covered entities to obtain an authorization for the use or disclosure of protected health information the covered entity creates for the purpose of research that includes treatment of individuals, except as otherwise permitted by § 164.512(i).

The intent of this provision is to permit covered entities that conduct research involving treatment to bind themselves to a more limited scope of uses and disclosures of research information than they would otherwise be permitted to make with non-research information. Rather than creating a single definition of ''research information,'' we allow covered entities the flexibility to define that subset of protected health information they create during clinical research that is not necessary for treatment, payment, or health care operations and that the covered entity will use or disclose under more limited circumstances than it uses or discloses other protected health information. In designing their authorizations, we expect covered entities to be mindful of the often highly sensitive nature of research information and the impact of individuals' privacy concerns on their willingness to participate in research.

Covered entities seeking authorization to use or disclose protected health information they create for the purpose of research that includes treatment of individuals, including clinical trials, must include in the authorization (in addition to the applicable elements required above) a description of the extent to which some or all of the protected health information created for the research will also be used or disclosed for purposes of treatment, payment, and health care operations. For example, if the covered entity intends to seek reimbursement from the individual's health plan for the routine costs of care associated with the research protocol, it must explain in the authorization the types of information that it will provide to the health plan for this purpose. This information, and the circumstances under which disclosures will be made for treatment, payment, and health care operations, may be more limited than the information and circumstances described in the covered entity's general consent and notice of privacy practices. To the extent the covered entity limits itself to a subset of uses or disclosures that are otherwise permissible under the rule and the covered entity's consent and notice, the covered entity is bound by the statements made in the research-related authorization. In these circumstances, the authorization must indicate that the authorization, not the general consent and notice, controls.

If the covered entity's primary interaction with the individual is through the research, the covered entity may combine the general consent for treatment, payment, and health care operations required under § 164.506 with this research authorization and need not obtain an additional consent under § 164.506. If the entity has already obtained, or intends to obtain, a separate consent as required under § 164.506, the research authorization must refer to that consent and state that the practices described in the research-related authorization are binding on the covered entity as to the information covered by the research-related authorization. The research-related authorization may also be combined in the same document as the informed consent for participation in the research. This is an exception to the general rule in § 164.508(b)(3) that an authorization under this section may not be combined with any other document (see above).

The covered entity must also include in the authorization a description of the extent to which it will not use or disclose the protected health information it obtains in connection with the research protocol for purposes that are permitted without individual authorization under this rule (under §§ 164.510 and 164.512). To the extent that the entity limits itself to a subset of uses or disclosures that are otherwise permissible under the rule and the entity's notice, the entity is bound by the statements made in the research authorization. In these circumstances, the authorization must indicate that the authorization, not the notice, controls. The covered entity may not, however, purport to preclude itself from making uses or disclosures that are required by law or that are necessary to avert a serious and imminent threat to health or safety.

In some instances, the covered entity may wish to make a use or disclosure of the research information that it did not include in its general consent or notice or for which authorization is required under this rule. To the extent the entity includes uses or disclosures in the research authorization that are otherwise not permissible under the rule and the entity's consent and notice of information practices, the entity must include all of the elements required by §§ 164.508(c) and (d) in the research-related authorization. The covered entity is bound by these statements.

Research that involves the delivery of treatment to participants sometimes relies on existing health information, such as to determine eligibility for the trial. We note that under § 164.508(b)(3)(iii), the covered entity may combine the research-related authorization required under § 164.508(f) with any other authorization for the use or disclosure of protected health information (other than psychotherapy notes), provided that the covered entity does not condition the provision of treatment on the individual signing the authorization. For example, a covered health care provider that had a treatment relationship with an individual prior to the individual's enrollment in a clinical trial, but that is now providing research-related treatment to the individual, may elect to request a compound authorization from the individual: an authorization under § 164.508(d) for the provider to use the protected health information it created prior to the initiation of the research that involves treatment, combined with an authorization under § 164.508(f) regarding use and disclosure of protected health information the covered provider will create for the purpose of the clinical trial. This compound authorization would be valid, provided the covered provider did not condition the research-related treatment on obtaining the authorization required under § 164.508(f), as permitted in § 164.508(b)(4)(i).

However, we anticipate that covered entities will almost always, if not always, condition the provision of research-related treatment on the individual signing the authorization under § 164.508(f) for the covered

entity's use or disclosure of protected health information created for the research. Therefore, we expect that the vast majority of covered providers who wish to use or disclose protected health information about an individual that will be created for research that includes treatment and wish to use existing protected health information about that individual for the research that includes treatment, will be required to obtain two authorizations from the individual: (1) an authorization for the use and disclosure of protected health information to be created for the research that involves treatment of the individual (as required under § 164.508(f)), and (2) an authorization for the use of existing protected health information for the research that includes treatment of the individual (as required under § 164.508(d)).

Effect of Authorization

As noted in the discussion about consents in the preamble to § 164.506, authorizations under this rule should not be construed to waive, directly or indirectly, any privilege granted under federal, state, or local laws or procedures.

Section 164.510—Uses and Disclosures Requiring an Opportunity for the Individual To Agree or To Object

Introduction

Section 164.510 of the NPRM proposed the uses and disclosures of protected health information that covered entities could make for purposes other than treatment, payment, or health care operations and for which an individual authorization would not have been required. These allowable uses and disclosures were designed to permit and promote key national health care priorities, and to promote the smooth operation of the health care system. In each of these areas, the proposal permitted, but would not have required, covered entities to use or disclose protected health information.

We proposed to require covered entities to obtain the individual's oral agreement before making a disclosure to a health care facility's directory or to the individual's next-of-kin or to another person involved in the individual's health care. Because there is an expectation in these two areas that individuals will have some input into a covered entity's decision to use or disclose protected health information, we decided to place disclosures to health facility directories and to persons involved in an individual's care in a separate section. In the final rule, requirements regarding disclosure of protected health information for facility directories and to others involved in an individual's care are included in § 164.510(a) and § 164.510(b), respectively. In the final rule, we include in § 164.510(b) provisions to address a type of disclosure not addressed in the NPRM: disclosures to entities providing relief and assistance in disasters such as floods, fires, and terrorist attacks. Requirements for most of the remaining categories of disclosures addressed in proposed § 164.510 of the NPRM are included in a new § 164.512 of the final rule, as discussed below.

Section 164.510 of the final rule addresses situations in which the interaction between the covered entity and the individual is relatively informal and agreements are made orally, without written authorizations for use or disclosure. In general, under the final rule, to disclose or use protected health information for these purposes, covered entities must inform individuals in advance and must provide a meaningful opportunity for the individual to prevent or restrict the disclosure. In exceptional circumstances, where even this informal discussion cannot practicably take place, covered entities are permitted to make decisions regarding disclosure or use based on the exercise of professional judgment of what is in the individual's best interest.

Section 164.510(a)—Use and Disclosure for Facility Directories

The NPRM proposed to allow covered health care providers to disclose through an inpatient facility's directory a patient's name, location in the facility, and general health condition, provided that the individual had agreed to the disclosure. The NPRM would have allowed this agreement to be oral. Pursuant to the NPRM, when making decisions about incapacitated individuals, a covered health care provider could have disclosed such information at the entity's discretion and consistent with good medical practice and any prior expressions of patient preference of which the covered entity was aware.

The preamble to the NPRM listed several factors that we encouraged covered entities to take into account when making decisions about whether to include an incapacitated patient's information in the directory. These factors included: (1) Whether disclosing that an individual is in the facility could reasonably cause harm or danger to the individual (*e.g.,* if it appeared that an unconscious patient had been abused and disclosing the information could give the attacker sufficient information to seek out the person and repeat the abuse); (2) whether disclosing a patient's location within a facility implicitly would give information about the patient's condition (*e.g.,* whether a patient's room number revealed that he or she was in a psychiatric ward); (3) whether it was necessary or appropriate to give information about patient status to family or friends (*e.g.,* if giving information to a family member about an unconscious patient could help a physician administer appropriate medications); and (4) whether an individual had, prior to becoming incapacitated, expressed a preference not to be included in the directory. The preamble stated that if a covered entity learned of such a preference, it would be required to act in accordance with the preference.

The preamble to the NPRM said that when individuals entered a facility in an incapacitated state and subsequently gained the ability to make their own decisions, health facilities should ask them within a reasonable time period for permission to include their information in the facility's directory.

In the final rule, we change the NPRM's opt-in authorization requirement to an opt-out approach for inclusion of patient information in a health care facility's directory. The final rule allows covered health care providers—which in this case are health care facilities—to include patient information in their directory only if: (1) They inform incoming patients of their policies regarding the directory; (2) they give patients a meaningful opportunity to opt out of the directory listing or to restrict some or all of the uses and disclosures that can be included in the directory; and (3) the patient does not object to being included in the directory. A patient must be allowed, for example, to have his or her name and condition included in the directory while not having his or her religious affiliation included. The facility's notice and the individual's opt-out or restriction may be oral.

Under the final rule, subject to the individual's right to object, or known prior expressed preferences, a covered health care provider may disclose the following information to persons who inquire about the individual by name: (1) The individual's general condition in terms that do not communicate specific medical information about the individual (*e.g.,* fair, critical, stable, *etc.*); and (2) location in the facility. This approach represents a slight change to the NPRM, which did not require members of the general public to ask for a patient by name in order to obtain directory information and which,

in fact, would have allowed covered entities to disclose the individual's name as part of directory information.

Under the final rule, we also establish provisions for disclosure of directory information to clergy that are slightly different from those which apply for disclosure to the general public. Subject to the individual's right to object or restrict the disclosure, the final rule permits a covered entity to disclose to a member of the clergy: (1) The individual's name; (2) the individual's general condition in terms that do not communicate specific medical information about the individual; (3) the individual's location in the facility; and (4) the individual's religious affiliation. A disclosure of directory information may be made to members of the clergy even if they do not inquire about an individual by name. We note that the rule in no way requires a covered health care provider to inquire about the religious affiliation of an individual, nor must individuals supply that information to the facility. Individuals are free to determine whether they want their religious affiliation disclosed to clergy through facility directories.

We believe that allowing clergy to access patient information pursuant to this section does not violate the Establishment Clause of the First Amendment, which prohibits laws ''respecting an establishment of religion.'' Courts traditionally turn to the Lemon test when evaluating laws that might raise Establishment Clause concerns. A law does not violate the Clause if it has a secular purpose, is not primarily to advance religion, and does not cause excessive government entanglement with religion. The privacy regulation passes this test because its purpose is to protect the privacy of individuals—regardless of their religious affiliation—and it does not cause excessive government entanglement.

More specifically, although this section provides a special rule for members of the clergy, it does so as an accommodation to patients who seek to engage in religious conduct. For example, restricting the disclosure of an individual's religious affiliation, room number, and health status to a priest could cause significant delay that would inhibit the ability of a Catholic patient to obtain sacraments provided during the last rites. We believe this accommodation does not violate the Establishment Clause, because it avoids a government-imposed restriction on the disclosure of information that could disproportionately affect the practice of religion. In that way, it is no different from accommodations upheld by the U.S. Supreme Court, such as exceptions to laws banning the use of alcohol in religious ceremonies.

The final rule expands the circumstances under which health care facilities can disclose specified health information to the patient directory without the patient's agreement. Besides allowing such disclosures when patients are incapacitated, as the NPRM would have allowed, the final rule allows such disclosures in emergency treatment circumstances. For example, when a patient is conscious and capable of making a decision, but is so seriously injured that asking permission to include his or her information in the directory would delay treatment such that the patient's health would be jeopardized, health facilities can make decisions about including the patient's information in the directory according to the same rules that apply when the patient is incapacitated. The final rule modifies the NPRM requirements for cases in which an incapacitated patient is admitted to a health care facility. Whereas the NPRM would have allowed health care providers to disclose an incapacitated patient's information to the facility's directory ''at its discretion and consistent with good medical practice and any prior expressions of preference of which the covered entity [was] aware,'' the final rule states that in these situations (and in other emergency treatment circumstances), covered health care providers must make the decision on whether to include the patient's information in the facility's directory in accordance with professional judgment as to the patient's best interest. In addition, when making decisions involving incapacitated patients and patients in emergency situations, covered health care providers may decide to include some portions of the patient's information (such as name) but not other information (such as location in the facility) in order to protect patient interests.

As in the preamble to the NPRM, we encourage covered health care providers to take into account the four factors listed above when making decisions about whether to include patient information in a health care facility's directory when patients are incapacitated or are in an emergency treatment circumstance. In addition, we retain the requirement stated in the preamble of the NPRM that if a covered health care provider learns of an incapacitated patient's prior expression of preference not to be included in a facility's directory, the facility must not include the patient's information in the directory. For cases involving patients admitted to a health care facility in an incapacitated or emergency treatment circumstance who during the course of their stay become capable of decisionmaking, the final rule takes an approach similar to that described in the NPRM. The final rule states that when an individual who was incapacitated or in an emergency treatment circumstance upon admission to an inpatient facility and whose condition stabilizes such that he or she is capable of decisionmaking, a covered health care provider must, when it becomes practicable, inform the individual about its policies regarding the facility's directory and provide the opportunity to object to the use or disclosure of protected health information about themselves for the directory.

Section 164.510(b)—Uses and Disclosures for Involvement in the Individual's Care and Notification Purposes

In cases involving an individual with the capacity to make health care decisions, the NPRM would have allowed covered entities to disclose protected health information about the individual to a next-of-kin, to other family members, or to close personal friends of the individual if the individual had agreed orally to such disclosure. If such agreement could not practicably or reasonably be obtained (*e.g.,* when the individual was incapacitated), the NPRM would have allowed disclosure of protected health information that was directly relevant to the person's involvement in the individual's health care, consistent with good health professional practices and ethics. The NPRM defined next-of-kin as defined under state law.

Under the final rule, we specify that covered entities may disclose to a person involved in the current health care of the individual (such as a family member, other relative, close personal friend, or any other person identified by the individual) protected health information directly related to the person's involvement in the current health care of an individual or payment related to the individual's health care. Such persons involved in care and other contact persons might include, for example: blood relatives; spouses; roommates; boyfriends and girlfriends; domestic partners; neighbors; and colleagues. Inclusion of this list is intended to be illustrative only, and it is not intended to change current practices with respect to: (1) Involvement of other persons in individuals' treatment decisions; (2) informal information-sharing among individuals involved in a person's care; or (3) sharing of protected health

information to contact persons during a disaster. The final rule also includes new language stating that covered entities may use or disclose protected health information to notify or assist in notification of family members, personal representatives, or other persons responsible for an individual's care with respect to an individual's location, condition, or death. These provisions allow, for example, covered entities to notify a patient's adult child that his father has suffered a stroke and to tell the person that the father is in the hospital's intensive care unit.

The final rule includes separate provisions for situations in which the individual is present and for when the individual is not present at the time of disclosure. When the individual is present and has the capacity to make his or her own decisions, a covered entity may disclose protected health information only if the covered entity: (1) Obtains the individual's agreement to disclose to the third parties involved in their care; (2) provides the individual with an opportunity to object to such disclosure and the individual does not express an objection; or (3) reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure. Situations in which covered providers may infer an individual's agreement to disclose protected health information pursuant to option (3) include, for example, when a patient brings a spouse into the doctor's office when treatment is being discussed, and when a colleague or friend has brought the individual to the emergency room for treatment.

We proposed that when a covered entity could not practicably obtain oral agreement to disclose protected health information to next-of-kin, relatives, or those with a close personal relationship to the individual, the covered entity could make such disclosures consistent with good health professional practice and ethics. In such instances, we proposed that covered entities could disclose only the minimum information necessary for the friend or relative to provide the assistance he or she was providing. For example, health care providers could not disclose to a friend or relative simply driving a patient home from the hospital extensive information about the patient's surgery or past medical history when the friend or relative had no need for this information.

The final rule takes a similar approach. Under the final rule, when an individual is not present (for example, when a friend of a patient seeks to pick up the patient's prescription at a pharmacy) or when the opportunity to agree or object to the use or disclosure cannot practicably be provided due to the individual's incapacity or an emergency circumstance, covered entities may, in the exercise of professional judgment, determine whether the disclosure is in the individual's best interests and if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's health care. For example, this provision allows covered entities to inform relatives or others involved in a patient's care, such as the person who accompanied the individual to the emergency room, that a patient has suffered a heart attack and to provide updates on the patient's progress and prognosis when the patient is incapacitated and unable to make decisions about such disclosures. In addition, this section allows covered entities to disclose functional information to individuals assisting in a patient's care; for example, it allows hospital staff to give information about a person's mobility limitations to a friend driving the patient home from the hospital. It also allows covered entities to use professional judgment and experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on an individual's behalf to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information. Thus, under this provision, pharmacists may release a prescription to a patient's friend who is picking up the prescription for him or her. Section 164.510(b) is not intended to disrupt most covered entities' current practices or state law with respect to these types of disclosures.

This provision is intended to allow disclosures directly related to a patient's current condition and should not be construed to allow, for example, disclosure of extensive information about the patient's medical history that is not relevant to the patient's current condition and that could prove embarrassing to the patient. In addition, if a covered entity suspects that an incapacitated patient is a victim of domestic violence and that a person seeking information about the patient may have abused the patient, covered entities should not disclose information to the suspected abuser if there is reason to believe that such a disclosure could cause the patient serious harm. In all of these situations regarding possible disclosures of protected health information about an patient who is not present or is unable to agree to such disclosures due to incapacity or other emergency circumstance, disclosures should be in accordance with the exercise of professional judgment as to the patient's best interest.

This section is not intended to provide a loophole for avoiding the rule's other requirements, and it is not intended to allow disclosures to a broad range of individuals, such as journalists who may be curious about a celebrity's health status. Rather, it should be construed narrowly, to allow disclosures to those with the closest relationships with the patient, such as family members, in circumstances when a patient is unable to agree to disclosure of his or her protected health information. Furthermore, when a covered entity cannot practicably obtain an individual's agreement before disclosing protected health information to a relative or to a person involved in the individual's care and is making decisions about such disclosures consistent with the exercise of professional judgment regarding the individual's best interest, covered entities must take into account whether such a disclosure is likely to put the individual at risk of serious harm.

Like the NPRM, the final rule does not require covered entities to verify the identity of relatives or other individuals involved in the individual's care. Rather, the individual's act of involving the other persons in his or her care suffices as verification of their identity. For example, the fact that a person brings a family member into the doctor's office when treatment information will be discussed constitutes verification of the involved person's identity for purposes of this rule. Likewise, the fact that a friend arrives at a pharmacy and asks to pick up a specific prescription for an individual effectively verifies that the friend is involved in the individual's care, and the rule allows the pharmacist to give the filled prescription to the friend.

We also clarify that the final rule does not allow covered entities to assume that an individual's agreement at one point in time to disclose protected health information to a relative or to another person assisting in the individual's care implies agreement to disclose protected health information indefinitely in the future. We encourage the exercise of professional judgment in determining the scope of the person's involvement in the individual's care and the time period for which the individual is agreeing to the other person's involvement. For example, if a friend simply picks up a patient from the hospital but has played no other role

in the individual's care, hospital staff should not call the friend to disclose lab test results a month after the initial encounter with the friend. However, if a patient routinely brings a spouse into the doctor's office when treatment is discussed, a physician can infer that the spouse is playing a long-term role in the patient's care, and the rule allows disclosure of protected health information to the spouse consistent with his or her role in the patient's care, for example, discussion of treatment options.

The NPRM did not specifically address situations in which disaster relief organizations may seek to obtain protected health information from covered entities to help coordinate the individual's care, or to notify family or friends of an individual's location or general condition in a disaster situation. In the final rule, we account for disaster situations in this paragraph. Specifically, we allow covered entities to use or disclose protected health information without individual agreement to federal, state, or local government agencies engaged in disaster relief activities, as well as to private disaster relief or disaster assistance organizations (such as the Red Cross) authorized by law or by their charters to assist in disaster relief efforts, to allow these organizations to carry out their responsibilities in a specific disaster situation. Covered entities may make these disclosures to disaster relief organizations, for example, so that these organizations can help family members, friends, or others involved in the individual's care to locate individuals affected by a disaster and to inform them of the individual's general health condition. This provision also allows disclosure of information to disaster relief or disaster assistance organizations so that these organizations can help individuals obtain needed medical care for injuries or other health conditions caused by a disaster.

We encourage disaster relief organizations to protect the privacy of individual health information to the extent practicable in a disaster situation. However, we recognize that the nature of disaster situations often makes it impossible or impracticable for disaster relief organizations and covered entities to seek individual agreement or authorization before disclosing protected health information necessary for providing disaster relief. Thus, we note that we do not intend to impede disaster relief organizations in their critical mission to save lives and reunite loved ones and friends in disaster situations.

Section 164.512—Uses and Disclosures for Which Consent, an Authorization, or Opportunity To Agree or Object Is Not Required

Introduction

The final rule's requirements regarding disclosures for directory information and to family members or others involved in an individual's care are in a section separate from that covering disclosures allowed for other national priority purposes. In the final rule, we place most of the other disclosures for national priority purposes in a new § 164.512.

As in the NPRM, in § 164.512 of the final rule, we allow covered entities to make these national priority uses and disclosures without individual authorization. As in the NPRM, these uses and disclosures are discretionary. Covered entities are free to decide whether or not to use or disclose protected health information for any or all of the permitted categories. However, as in the NPRM, nothing in the final rule provides authority for a covered entity to restrict or refuse to make a use or disclosure mandated by other law.

The new § 164.512 includes paragraphs on: Uses and disclosures required by law; uses and disclosures for public health activities; disclosures about victims of abuse, neglect, or domestic violence; uses and disclosures for health oversight activities; disclosures for judicial and administrative proceedings; disclosures for law enforcement purposes; uses and disclosures about decedents; uses and disclosures for cadaveric donation of organs, eyes, or tissues; uses and disclosures for research purposes; uses and disclosures to avert a serious threat to health or safety (which we had called ''emergency circumstances'' in the NPRM); uses and disclosures for specialized government functions (referred to as ''specialized classes'' in the NPRM); and disclosures to comply with workers' compensation laws.

Section 164.512(c) in the final rule, which addresses uses and disclosures regarding adult victims of abuse, neglect and domestic violence, is new, although it incorporates some provisions from proposed § 164.510 of the NPRM. In the final rule we also eliminate proposed § 164.510(g) on government health data systems and proposed § 164.510(i) on banking and payment processes. These changes are discussed below.

Approach to Use of Protected Health Information

Proposed § 164.510 of the NPRM included specific subparagraphs addressing uses of protected health information by covered entities that were also public health agencies, health oversight agencies, government entities conducting judicial or administrative proceedings, or government heath data systems. Such covered entities could use protected health information in all instances for which they could disclose the information for these purposes. In the final rule, as discussed below, we retain this language in the paragraphs on public health activities and health oversight. However, we eliminate this clause with respect to uses of protected health information for judicial and administrative proceedings, because we no longer believe that there would be any situations in which a covered entity would also be a judicial or administrative tribunal. Proposed § 164.510(e) of the NPRM, regarding disclosure of protected health information to coroners, did not include such a provision. In the final rule we have added it because we believe there are situations in which a covered entity, for example, a public hospital conducting post-mortem investigations, may need to use protected health information for the same purposes for which it would have disclosed the information to a coroner.

While the right to request restrictions under § 164.522 and the consents required under § 164.506 do not apply to the use and disclosure of protected health information under § 164.512, we do not intend to preempt any state or other restrictions, or any right to enforce such agreements or consents under other law.

We note that a covered entity may use or disclose protected health information as permitted by and in accordance with one of the paragraphs of § 164.512, regardless of whether that use or disclosure fails to meet the requirements for use or disclosure under a different paragraph in § 164.512 or elsewhere in the rule.

Verification for Disclosures Under § 164.512

In § 164.510(a) of the NPRM, we proposed that covered entities verify the identity and authority of persons to whom they made disclosure under the section. In the final rule, we generally have retained the proposed requirements. Verification requirements are discussed in § 164.514 of the final rule.

Section 164.512(a)—Uses and Disclosures Required by Law

In the NPRM we would have allowed covered entities to use or disclose protected health information without individual authorization where such use

or disclosure was required by other law, as long as the use or disclosure met all relevant requirements of such law. However, a legally mandated use or disclosure which fell into one or more of the national priority purposes expressly identified in proposed § 164.510 of the NPRM would have been subject to the terms and conditions specified by the applicable paragraph of proposed § 164.510. Thus, a disclosure required by law would have been allowed only to the extent it was not otherwise prohibited or restricted by another provision in proposed § 164.510. For example, mandatory reporting to law enforcement officials would not have been allowed unless such disclosures conformed to the requirements of proposed § 164.510(f) of the NPRM, on uses and disclosures for law enforcement purposes. As explained in the NPRM, this provision was not intended to obstruct access to information deemed important enough by federal, state or other government authorities to require it by law.

In § 164.512(a) of the final rule, we retain the proposed approach, and we permit covered entities to comply with laws requiring the use or disclosure of protected health information, provided the use or disclosure meets and is limited to the relevant requirements of such other laws. To more clearly address where the substantive and procedural requirements of other provisions in this section apply, we have deleted the general sentence from the NPRM which stated that the provision ''does not apply to uses or disclosures that are covered by paragraphs (b) through (m)'' of proposed § 164.510. Instead, in § 164.512 (a)(2) we list the specific paragraphs that have additional requirements with which covered entities must comply. They are disclosures about victims of abuse, neglect or domestic violence (§ 164.512(c)), for judicial and administrative proceedings (§ 164.512(e)), and for law enforcement purposes (§ 164.512(f)). We include a new definition of ''required by law.'' See § 164.501. We clarify that the requirements provided for in § 164.514(h) relating to verification apply to disclosures under this paragraph. Those provisions require covered entities to verify the identity and authority of persons to whom they make disclosures. We note that the minimum necessary requirements of § 164.514(d) do not apply to disclosures made under this paragraph.

We note that this rule does not affect what is required by other law, nor does it compel a covered entity to make a use or disclosure of protected health information required by the legal demands or reporting requirements listed in the definition of ''required by law.'' Covered entities will not be sanctioned under this rule for responding in good faith to such legal process and reporting requirements. However, nothing in this rule affects, either by expanding or contracting, a covered entity's right to challenge such process or reporting requirements under other laws. The only disclosures of protected health information compelled by this rule are disclosures to an individual (or the personal representative of an individual) or to the Secretary for the purposes of enforcing this rule.

Uses and disclosures permitted under this paragraph must be limited to the protected health information necessary to meet the requirements of the law that compels the use or disclosure. For example, disclosures pursuant to an administrative subpoena are limited to the protected health information authorized to be disclosed on the face of the subpoena.

Section 164.512(b)—Uses and Disclosures for Public Health Activities

The NPRM would have allowed covered entities to disclose protected health information without individual authorization to: (1) A public health authority authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; (2) a public health authority or other appropriate authority authorized by law to receive reports of child abuse or neglect; (3) a person or entity other than a governmental authority that could demonstrate or demonstrated that it was acting to comply with requirements or direction of a public health authority; or (4) a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition and was authorized by law to be notified as necessary in the conduct of a public health intervention or investigation.

In the final rule, we broaden the scope of permissible disclosures pursuant to item (1) listed above. We narrow the scope of disclosures permissible under item (3) of this list, and we add language to clarify the scope of permissible disclosures with respect to item (4) on the list. We broaden the scope of allowable disclosures regarding item (1) by allowing covered entities to disclose protected health information not only to U.S. public health authorities but also, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority. For example, we allow covered entities to disclose protected health information to a foreign government agency that is collaborating with the Centers for Disease Control and Prevention to limit the spread of infectious disease.

We narrow the conditions under which covered entities may disclose protected health information to non-government entities. We allow covered entities to disclose protected health information to a person subject to the FDA's jurisdiction, for the following activities: to report adverse events (or similar reports with respect to food or dietary supplements), product defects or problems, or biological product deviations, if the disclosure is made to the person required or directed to report such information to the FDA; to track products if the disclosure is made to a person required or directed by the FDA to track the product; to enable product recalls, repairs, or replacement, including locating and notifying individuals who have received products regarding product recalls, withdrawals, or other problems; or to conduct post-marketing surveillance to comply with requirements or at the direction of the FDA.

The terms included in § 164.512(b)(iii) are intended to have both their commonly understood meanings, as well as any specialized meanings, pursuant to the Food, Drug, and Cosmetic Act (21 U.S.C. 321 *et seq.*) or the Public Health Service Act (42 U.S.C. 201 *et seq.*). For example, ''post-marketing surveillance'' is intended to mean activities related to determining the safety or effectiveness of a product after it has been approved and is in commercial distribution, as well as certain Phase IV (post-approval) commitments by pharmaceutical companies. With respect to devices, ''post-marketing surveillance'' can be construed to refer to requirements of section 522 of the Food, Drug, and Cosmetic Act regarding certain implanted, life-sustaining, or life-supporting devices. The term ''track'' includes, for example, tracking devices under section 519(e) of the Food, Drug, and Cosmetic Act, units of blood or other blood products, as well as trace-backs of contaminated food.

In § 164.512(b)(iii), the term ''required'' refers to requirements in statute, regulation, order, or other

legally binding authority exercised by the FDA. The term ''directed,'' as used in this section, includes other official agency communications such as guidance documents.

We note that under this provision, a covered entity may disclose protected health information to a non-governmental organization without individual authorization for inclusion in a private data base or registry only if the disclosure is otherwise for one of the purposes described in this provision (*e.g.,* for tracking products pursuant to FDA direction or requirements, for post-marketing surveillance to comply with FDA requirements or direction.)

To make a disclosure that is not for one of these activities, covered entities must obtain individual authorization or must meet the requirements of another provision of this rule. For example, covered entities may disclose protected health information to employers for inclusion in a workplace surveillance database only: with individual authorization; if the disclosure is required by law; if the disclosure meets the requirements of § 164.512(b)(v); or if the disclosure meets the conditions of another provision of this regulation, such as § 154.512(i) relating to research. Similarly, if a pharmaceutical company seeks to create a registry containing protected health information about individuals who had taken a drug that the pharmaceutical company had developed, covered entities may disclose protected health information without authorization to the pharmaceutical company pursuant to FDA requirements or direction. If the pharmaceutical company's registry is not for any of these purposes, covered entities may disclose protected health information to it only with patient authorization, if required by law, or if disclosure meets the conditions of another provision of this rule.

The final rule continues to permit covered entities to disclose protected health information without individual authorization directly to public health authorities, such as the Food and Drug Administration, the Occupational Safety and Health Administration, the Centers for Disease Control and Prevention, as well as state and local public health departments, for public health purposes as specified in the NPRM.

The final rule retains the NPRM provision allowing covered entities to disclose protected health information to public health authorities or other appropriate government authorities authorized by law to receive reports of child abuse or neglect. In addition, we clarify the NPRM's provision regarding disclosure of protected health information to persons who may have been exposed to a communicable disease or who may otherwise be at risk of contracting or spreading a disease or condition. Under the final rule, covered entities may disclose protected health information to such individuals when the covered entity or public health authority is authorized by law to notify these individuals as necessary in the conduct of a public health intervention or investigation.

In addition, as in the NPRM, under the final rule, a covered entity that is acting as a public health authority—for example, a public hospital conducting infectious disease surveillance in its role as an arm of the public health department—may use protected health information in all cases for which it is allowed to disclose such information for public health activities as described above.

The proposed rule did not contain a specific provision relating to disclosures by covered health care providers to employers concerning work-related injuries or illnesses or workplace medical surveillance. Under the proposed rule, a covered entity would have been permitted to disclose protected health information without individual authorization for public health purposes to private person if the person could demonstrate that it was acting to comply with requirements or at the direction of a public health authority.

As discussed above, in the final rule we narrow the scope of this paragraph as it applies to disclosures to persons other than public health authorities. To ensure that covered health care providers may make disclosures of protected health information without individual authorization to employers when appropriate under federal and state laws addressing work-related injuries and illnesses or workplace medical surveillance, we include a new provision in the final rule. The provision permits covered health care providers who provide health care as a workforce member of or at the request of an employer to disclose to that employer protected health information concerning work-related injuries or illnesses or workplace medical surveillance in situations where the employer has a duty under the Occupational Safety and Health Act, the Federal Mine Safety and Health Act, or under a similar state law, to keep records on or act on such information. For example, OSHA regulations in 29 CFR part 1904 require employers to record work-related injuries and illnesses if medical treatment is necessary; MSHA regulations at 30 CFR part 50 require mine operators to report injuries and illnesses experienced by miners. Similarly, OSHA rules require employers to monitor employees' exposure to certain substances and to remove employees from exposure when toxic thresholds have been met. To obtain the relevant health information necessary to determine whether an injury or illness should be recorded, or whether an employee must be medically removed from exposure at work, employers must refer employees to health care providers for examination and testing.

OSHA and MSHA rules do not impose duties directly upon health care providers to disclose health information pertaining to recordkeeping and medical monitoring requirements to employers. Rather, these rules operate on the presumption that health care providers who provide services at the request of an employer will be able to disclose to the employer work-related health information necessary for the employer to fulfill its compliance obligations. This new provision permits covered entities to make disclosures necessary for the effective functioning of OSHA and MSHA requirements, or those of similar state laws, by permitting a health care provider to make disclosures without the authorization of the individual concerning work-related injuries or illnesses or workplace medical surveillance in situations where the employer has a duty under OSHA and MSHA requirements, or under a similar state laws, to keep records on or act on such information.

We require health care providers who make disclosures to employers under this provision to provide notice to individuals that it discloses protected health information to employers relating to the medical surveillance of the workplace and work-related illnesses and injuries. The notice required under this provision is separate from the notice required under § 164.520. The notice required under this provision may be met giving a copy of the notice to the individual at the time it provides the health care services, or, if the health care services are provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care services are provided.

This provision applies only when a covered health care provider provides health care services as a workforce member of or at the request of an employer and for the purposes discussed above. The provision does not affect the application of this rule to other health care provided to

individuals or to their relationship with health care providers that they select.

Section 164.512(c)—Disclosures About Victims of Abuse, Neglect or Domestic Violence

The NPRM included two provisions related to disclosures about persons who are victims of abuse. In the NPRM, we would have allowed covered entities to report child abuse to a public health authority or other appropriate authority authorized by law to receive reports of child abuse or neglect. In addition, under proposed § 164.510(f)(3) of the NPRM, we would have allowed covered entities to disclose protected health information about a victim of a crime, abuse or other harm to a law enforcement official under certain circumstances. The NPRM recognized that most, if not all, states had laws that mandated reporting of child abuse or neglect to the appropriate authorities. Moreover, HIPAA expressly carved out state laws on child abuse and neglect from preemption or any other interference. The NPRM further acknowledged that most, but not all, states had laws mandating the reporting of abuse, neglect or exploitation of the elderly or other vulnerable adults. We did not intend to impede reporting in compliance with these laws.

The final rule includes a new paragraph, § 164.512(c), which allows covered entities to report protected health information to specified authorities in abuse situations other than those involving child abuse and neglect. In the final rule, disclosures of protected health information related to child abuse continues to be addressed in the paragraph allowing disclosure for public health activities (§ 164.512(b)), as described above. Because HIPAA addresses child abuse specifically in connection with a state's public health activities, we believe it would not be appropriate to include child abuse-related disclosures in this separate paragraph on abuse. State laws continue to apply with respect to child abuse, and the final rule does not in any way interfere with a covered entity's ability to comply with these laws.

In the final rule, we address disclosures about other victims of abuse, neglect and domestic violence in § 164.512(c) rather than in the law enforcement paragraph. Section 164.512(c) establishes conditions for disclosure of protected health information in cases involving domestic violence other than child abuse (*e.g.,* spousal abuse), as well as those involving abuse or neglect (*e.g.,* abuse of nursing home residents or residents of facilities for the mentally retarded). This paragraph addresses reports to law enforcement as well as to other authorized public officials. The provisions of this paragraph supersede the provisions of § 164.512(a) and § 164.512(f)(1)(i) to the extent that those provisions address the subject matter of this paragraph.

Under the circumstances described below, the final rule allows covered entities to disclose protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence. In this paragraph, references to ''individual'' should be construed to mean the individual believed to be the victim. The rule allows such disclosure to any governmental authority authorized by law to receive reports of such abuse, neglect, or domestic violence. These entities may include, for example, adult protective or social services agencies, state survey and certification agencies, ombudsmen for the aging or those in long-term care facilities, and law enforcement or oversight.

The final rule specifies three circumstances in which disclosures of protected health information is allowed in order to report abuse, neglect or domestic violence. First, this paragraph allows disclosure of protected health information related to abuse if required by law and the disclosure complies with and is limited to the relevant requirements of such law. As discussed below, the final rule requires covered entities that make such disclosures pursuant to a state's mandatory reporting law to inform the individual of the report.

Second, this paragraph allows covered entities to disclose protected health information related to abuse if the individual has agrees to such disclosure. When considering the possibility of disclosing protected health information in an abuse situation pursuant to this section, we encourage covered entities to seek the individual's agreement whenever possible.

Third, this paragraph allows covered entities to disclose protected health information about an individual without the individual's agreement if the disclosure is expressly authorized by statute or regulation and either: (1) The covered entity, in the exercise of its professional judgment, believes that the disclosure is necessary to prevent serious harm to the individual or to other potential victims; or (2) if the individual is unable to agree due to incapacity, a law enforcement or other public official authorized to received the report represents that the protected health information for which disclosure is sought is not intended to be used against the individual, and that an immediate enforcement activity that depends on the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

We emphasize that disclosure under this third part of the paragraph also may be made only if it is expressly authorized by statute or regulation. We use this formulation, rather than the broader ''required by law,'' because of the heightened privacy and safety concerns in these situations. We believe it appropriate to defer to other public determinations regarding reporting of this information only where a legislative or executive body has determined the reporting to be of sufficient importance to warrant enactment of a law or promulgation of a regulation. Law and regulations reflect a clear decision to authorize the particular disclosure of protected health information, and reflect greater public accountability (*e.g.,* through the required public comment process or because enacted by elected representatives).

For example, a Wisconsin law (Wis. Stat § 46.90(4)) states that any person may report to a county agency or state official that he or she believes that abuse or neglect has occurred. Pursuant to § 164.512(c)(1)(iii), a covered entity may make a report only if the specific type or subject matter of the report (*e.g.,* abuse or neglect of the elderly) is included in the law authorizing the report, and such a disclosure may only be made to a public authority specifically identified in the law authorizing the report. Furthermore, we note that disclosures under this part of the paragraph are further limited to two circumstances. In the first case, a covered entity, in the exercise of professional judgment, must believe that the disclosure is necessary to prevent serious harm to the individual or to other potential victims. The second case addresses situations in which an individual who is a victim of abuse, neglect or domestic violence is unable to agree due to incapacity and a law enforcement or other public official authorized to receive the report represents that the protected health information for which disclosure is sought is not intended to be used against the individual and that an immediate law enforcement activity that depends on the disclosure would be materially and adversely affected by waiting until the individual if able to agree to the disclosure. We note that, in this second case, a covered entity may exercise discretion, consistent with professional judgment as to the patient's

best interest, in deciding whether to make the requested disclosure.

The rules governing disclosure in this third set of circumstances are different from those governing disclosures pursuant to § 164.512(f)(3) regarding disclosure to law enforcement about victims of crime and other harm. We believe that in abuse situations—to a greater extent than in situations involving crime victims in general—there is clear potential for abusers to cause further serious harm to the victim or to others, such as other family members in a household or other residents of a nursing home. The provisions allowing reporting of abuse when authorized by state law, as described above, are consistent with principles articulated by the AMA's Council on Ethical and Judicial Affairs, which state that when reporting abuse is voluntary under state law, it is justified when necessary to prevent serious harm to a patient. Through the provisions of § 164.512(c), we recognize the unique circumstances surrounding abuse and domestic violence, and we seek to provide an appropriate balance between individual privacy interests and important societal interests such as preventing serious harm to other individuals. We note that here we are relying on covered entities, in the exercise of professional judgment, to determine what is in the best interests of the patient.

Finally, we require covered entities to inform the individual in all of the situations described above that the covered entity has disclosed protected health information to report abuse, neglect, or domestic violence. We allow covered entities to provide this information orally. We do not require written notification, nor do we encourage it, due to the sensitivity of abuse situations and the potential for the abuser to cause further harm to the individual if, for example, a covered entity sends written notification to the home of the individual and the abuser. Whenever possible, covered entities should inform the individual at the same time that they determine abuse has occurred and decide that the abuse should be reported. In cases involving patient incapacity, we encourage covered entities to inform the individual of such disclosures as soon as it is practicable to do so.

The rule provides two exceptions to the requirement to inform the victim about a report to a government authority, one based on concern for future harm and one based on past harm. First, a covered entity need not inform the victim if the covered entity, in the exercise of professional judgment, believes that informing the individual would place the individual at risk of serious harm. We believe that this exception is necessary to address the potential for future harm, either physical or emotional, that the individual may face from knowing that the report has been made. Second, a covered entity may choose not to meet the requirement for informing the victim, if the covered entity actually would be informing a personal representative (such as a parent of a minor) and the covered entity reasonably believes that such person is responsible for the abuse, neglect, or other injury that has already occurred and that informing that person would not be in the individual's best interests.

Section 164.512(d)—Uses and Disclosures for Health Oversight Activities

Under § 164.510(c) of the NPRM, we proposed to permit covered entities to disclose protected health information to health oversight agencies for oversight activities authorized by law, including audit, investigation, inspection, civil, criminal, or administrative proceeding or action, or other activity necessary for appropriate oversight of: (i) the health care system; (ii) government benefit programs for which health information is relevant to beneficiary eligibility; or (iii) government regulatory programs for which health information is necessary for determining compliance with program standards.

In § 164.512(d) of the final rule, we modify the proposed language to include civil and criminal investigations. In describing ''other activities necessary for oversight'' of particular entities, we add the phrase ''entities subject to civil rights laws for which health information is necessary for determining compliance.'' In addition, in the final rule, we add ''licensure or disciplinary actions'' to the list of oversight activities authorized by law for which covered entities may disclose protected health information to health oversight agencies. The NPRM's definition of ''health oversight agency'' (in proposed § 164.504) included this phrase, but it was inadvertently excluded from the regulation text at proposed § 164.510(c). We make this change in the regulation text of the final rule to conform to the NPRM's definition of health oversight agency and to reflect the full range of activities for which we intend to allow covered entities to disclose protected health information to health oversight agencies.

The NPRM would have allowed, but would not have required, covered entities to disclose protected health information to public oversight agencies and to private entities acting under grant of authority from or under contract with oversight agencies for oversight purposes without individual authorization for health oversight activities authorized by law. When a covered entity was also an oversight agency, it also would have been permitted to use protected health information in all cases in which it would have been allowed to disclose such information for health oversight purposes. The NPRM would not have established any new administrative or judicial process prior to disclosure for health oversight, nor would it have permitted disclosures forbidden by other law. The proposed rule also would not have created any new right of access to health records by oversight agencies, and it could not have been used as authority to obtain records not otherwise legally available to the oversight agency.

The final rule retains this approach to health oversight. As in the NPRM, the final rule provides that when a covered entity is also an oversight agency, it is allowed to use protected health information in all cases in which it is allowed to disclose such information for health oversight purposes. For example, if a state insurance department is acting as a health plan in operating the state's Medicaid managed care program, the final rule allows the insurance department to use protected health information in all cases for which the plan can disclose the protected health information for health oversight purposes. For example, the state insurance department in its capacity as the state Medicaid managed care plan can use protected health information in the process of investigating and disciplining a state Medicaid provider for attempting to defraud the Medicaid system. As in the NPRM, the final rule does not establish any new administrative or judicial process prior to disclosure for health oversight, nor does it prohibit covered entities from making any disclosures for health oversight that are otherwise required by law. Like the NPRM, it does not create any new right of access to health records by oversight agencies and it cannot be used as authority to obtain records not otherwise legally available to the oversight agency.

Overlap Between Law Enforcement and Oversight

Under the NPRM, the proposed definitions of law enforcement and oversight, and the rules governing disclosures for these purposes

overlapped. Specifically, this overlap occurred because: (1) The NPRM preamble, but not the NPRM regulation text, indicated that agencies conducting both oversight and law enforcement activities would be subject to the oversight requirements when conducting oversight activities; and (2) the NPRM addressed some disclosures for investigations of health care fraud in the law enforcement paragraph (proposed § 164.510(f)(5)(i)), while health care fraud investigations are central to the purpose of health care oversight agencies (covered under proposed § 164.510(c)). In the final rule, we make substantial changes to these provisions, in an attempt to prevent confusion.

In § 164.512(d)(2), we include explicit decision rules indicating when an investigation is considered law enforcement and when an investigation is considered oversight under this regulation. An investigation or activity is not considered health oversight for purposes of this rule if: (1) The individual is the subject of the investigation or activity; and (2) The investigation or activity does not arise out of and is not directly related to: (a) The receipt of health care; (b) a claim for public benefits related to health; or (c) qualification for, or receipt of public benefits or services where a patient's health is integral to the claim for benefits or services. In such cases, where the individual is the subject of the investigation and the investigation does not relate to issues (a) through (c), the rules regarding disclosure for law enforcement purposes (see § 164.512(f)) apply. For the purposes of this rule, we intend for investigations regarding issues (a) through (c) above to mean investigations of health care fraud.

Where the individual is not the subject of the activity or investigation, or where the investigation or activity relates to the subject matter in (a) through (c) of the preceding sentence, a covered entity may make a disclosure pursuant to § 164.512(d)(1). For example, when the U.S. Department of Labor's Pension and Welfare Benefits Administration (PWBA) needs to analyze protected health information about health plan enrollees in order to conduct an audit or investigation of the health plan (*i.e.,* the enrollees are not subjects of the investigation) to investigate potential fraud by the plan, the health plan may disclose protected health information to the PWBA under the health oversight rules. These rules and distinctions are discussed in greater detail in our responses to comments.

To clarify further that health oversight disclosure rules apply generally in health care fraud investigations (subject to the exception described above), in the final rule, we eliminate proposed § 164.510(f)(5)(i), which would have established requirements for disclosure related to health care fraud for law enforcement purposes. All disclosures of protected health information that would have been permitted under proposed § 164.510(f)(5)(i) are permitted under § 164.512(d).

In the final rule, we add new language (§ 164.512(d)(3)) to address situations in which health oversight activities are conducted in conjunction with an investigation regarding a claim for public benefits not related to health (*e.g.,* claims for Food Stamps). In such situations, for example, when a state Medicaid agency is working with the Food Stamps program to investigate suspected fraud involving Medicaid and Food Stamps, covered entities may disclose protected health information to the entities conducting the joint investigation under the health oversight provisions of the rule.

In the proposed rule, the definitions of ''law enforcement proceeding'' and ''oversight activity'' both included the phrase ''criminal, civil, or administrative proceeding.'' For reasons explained below, the final rule retains this phrase in both definitions. The final rule does not attempt to distinguish between these activities based on the agency undertaking them or the applicable enforcement procedures. Rather, as described above, the final rule carves out certain activities which must always be considered law enforcement for purposes of disclosure of protected health information under this rule.

Additional Considerations

We note that covered entities are permitted to initiate disclosures that are permitted under this paragraph. For example, a covered entity could disclose protected health information in the course of reporting suspected health care fraud to a health oversight agency.

We delete language in the NPRM that would have allowed disclosure under this section only to law enforcement officials conducting or supervising an investigation, official inquiry, or a criminal, civil or administrative proceeding authorized by law. In some instances, a disclosure by a covered entity under this section will initiate such an investigation or proceeding, but it will not already be ongoing at the time the disclosure is made.

Section 164.512(e)—Disclosures and Uses for Judicial and Administrative Proceedings

Section 164.512(e) addresses when a covered entity is permitted to disclose protected health information in response to requests for protected health information that are made in the course of judicial and administrative proceedings—for example, when a non-party health care provider receives a subpoena (under Federal Rule of Civil Procedure Rule 45 or similar provision) for medical records from a party to a law suit. In the NPRM we would have allowed covered entities to disclose protected health information in the course of any judicial or administrative proceeding: (1) In response to an order of a court or administrative tribunal; or (2) where an individual was a party to the proceeding and his or her medical condition or history was at issue and the disclosure was pursuant to lawful process or otherwise authorized by law. Under the NPRM, if the request for disclosure of protected health information was accompanied by a court order, a covered entity could have disclosed that protected health information which the court order authorized to be disclosed. If the request for disclosure of protected health information were not accompanied by a court order, covered entities could not have disclosed the information requested unless a request authorized by law had been made by the agency requesting the information or by legal counsel representing a party to litigation, with a written statement certifying that the protected health information requested concerned a litigant to the proceeding and that the health condition of the litigant was at issue at the proceeding.

In § 164.512(e) of the final rule, we permit covered entities to disclose protected health information in a judicial or administrative proceeding if the request for such protected health information is made through or pursuant to an order from a court or administrative tribunal or in response to a subpoena or discovery request from, or other lawful process by a party to the proceeding. When a request is made pursuant to an order from a court or administrative tribunal, a covered entity may disclose the information requested without additional process. For example, a subpoena issued by a court constitutes a disclosure which is required by law as defined in this rule, and nothing in this rule is intended to interfere with the ability of the covered entity to comply with such subpoena.

However, absent an order of, or a subpoena issued by, a court or administrative tribunal, a covered entity may respond to a subpoena or discovery request from, or other lawful process by, a party to the proceeding only if the covered entity obtains either: (1) Satisfactory assurances that reasonable efforts have been made to give the individual whose information has been requested notice of the request; or (2) satisfactory assurances that the party seeking such information has made reasonable efforts to secure a protective order that will guard the confidentiality of the information. In meeting the first test, a covered entity is considered to have received satisfactory assurances from the party seeking the information if that party demonstrates that it has made a good faith effort (such as by sending a notice to the individual's last known address) to provide written notice to the individual whose information is the subject of the request, that the written notice included sufficient information about the proceeding to permit the individual to raise an objection, and that the time for the individual to raise objections to the court or administrative tribunal has elapsed and no objections were filed or any objections filed by the individual have been resolved.

Unless required to do so by other law, the covered entity is not required to explain the procedures (if any) available for the individual to object to the disclosure. Under the rule, the individual exercises the right to object before the court or other body having jurisdiction over the proceeding, and not to the covered entity. The provisions in this paragraph are not intended to disrupt current practice whereby an individual who is a party to a proceeding and has put his or her medical condition at issue will not prevail without consenting to the production of his or her protected health information. In such cases, we presume that parties will have ample notice and an opportunity to object in the context of the proceeding in which the individual is a party.

As described above, in this paragraph we also permit a covered entity to disclose protected health information in response to a subpoena, discovery request, or other lawful process if the covered entity receives satisfactory assurances that the party seeking the information has made reasonable efforts to seek a qualified protective order that would protect the privacy of the information. A ''qualified protective order'' means an order of a court or of an administrative tribunal or a stipulation that: (1) Prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which the records are requested; and (2) requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding. Satisfactory assurances of reasonable efforts to secure a qualified protective order are a statement and documentation that the parties to the dispute have agreed to a protective order and that it has been submitted to the court or administrative tribunal with jurisdiction, or that the party seeking the protected health information has requested a qualified protective order from such court or tribunal. We encourage the development of ''model'' protective orders that will facilitate adherence with this subpart.

In the final rule we also permit the covered entity itself to satisfy the requirement to make reasonable efforts to notify the individual whose information has been requested or to seek a qualified protective order. We intend this to be a permissible activity for covered entities: we do not require covered entities to undertake these efforts in response to a subpoena, discovery request, or similar process (other than an order from a court or administrative tribunal). If a covered entity receives such a request without receiving the satisfactory assurances described above from the party requesting the information, the covered entity is free to object to the disclosure and is not required to undertake the reasonable efforts itself.

We clarify that the provisions of this paragraph do not supersede or otherwise invalidate other provisions of this rule that permit uses and disclosures of protected health information. For example, the fact that protected health information is the subject of a matter before a court or tribunal does not prevent its disclosure under another provision of the rule, such as §§ 164.512(b), 164.512(d), or 164.512(f), even if a public agency's method of requesting the information is pursuant to an administrative proceeding. For example, where a public agency commences a disciplinary action against a health professional, and requests protected health information as part of its investigation, the disclosure made be made to the agency under paragraph (d) of this section (relating to health oversight) even if the method of making the request is through the proceeding. As with any request for disclosure under this section, the covered entity will need to verify the authority under which the request is being made, and we expect that public agencies will identify their authority when making such requests. We note that covered entities may reasonably rely on assertions of authority made by government agencies.

Additional Considerations

Where a disclosure made pursuant to this paragraph is required by law, such as in the case of an order from a court or administrative tribunal, the minimum necessary requirements in § 164.514(d) do not apply to disclosures made under this paragraph. A covered entity making a disclosure under this paragraph, however, may of course disclose only that protected health information that is within the scope of the permitted disclosure. For instance, in response to an order of a court or administrative tribunal, the covered entity may disclose only the protected health information that is expressly authorized by such an order. Where a disclosure is not considered under this rule to be required by law, the minimum necessary requirements apply, and the covered entity must make reasonable efforts to limit the information disclosed to that which is reasonably necessary to fulfill the request. A covered entity is not required to second guess the scope or purpose of the request, or take action to resist the request because they believe that it is over broad. In complying with the request, however, the covered entity must make reasonable efforts not to disclose more information than is requested. For example, a covered entity may not provide a party free access to its medical records under the theory that the party can identify the information necessary for the request. In some instances, it may be appropriate for a covered entity, presented with a relatively broad discovery request, to permit access to a relatively large amount of information in order for a party to identify the relevant information. This is permissible as long as the covered entity makes reasonable efforts to circumscribe the access as appropriate.

The NPRM indicated that when a covered entity was itself a government agency, the covered entity could use protected health information in all cases in which it would have been allowed to disclose such information in the course of any judicial or administrative proceeding. As explained above, the final rule does not include this provision.

Section 164.512(f)—Disclosure for Law Enforcement Purposes

Disclosures Pursuant to Process and as Otherwise Required by Law

In the NPRM we would have allowed covered entities to disclose protected health information without individual authorization as required by other law. However, as explained above, if a legally mandated use or disclosure fell into one or more of the national priority purposes expressly identified in other paragraphs of proposed § 164.510, the disclosure would have been subject to the terms and conditions specified by the applicable paragraph of proposed § 164.510. For example, mandatory reporting to law enforcement officials would not have been allowed unless such disclosures conformed to the requirements of proposed § 164.510(f) of the NPRM. Proposed § 164.510(f) did not explicitly recognize disclosures required by other laws, and it would not have permitted covered entities to comply with some state and other mandatory reporting laws that require covered entities to disclose protected health information to law enforcement officials, such as the reporting of gun shot wounds, stab wounds, and/or burn injuries.

We did not intend to preempt generally state and other mandatory reporting laws, and in § 164.512(f)(1)(i) of the final rule, we explicitly permit covered entities to disclose protected health information for law enforcement purposes as required by other law. This provision permits covered entities to comply with these state and other laws. Under this provision, to the extent that a mandatory reporting law falls under the provisions of § 164.512(c)(1)(i) regarding reporting of abuse, neglect, or domestic violence, the requirements of those provisions supersede.

In the final rule, we specify that covered entities may disclose protected health information pursuant to this provision in compliance with and as limited by the relevant requirements of legal process or other law. In the NPRM, for the purposes of this portion of the law enforcement paragraph, we proposed to define ''law enforcement inquiry or proceeding'' as an investigation or official proceeding inquiring into a violation of or failure to comply with law; or a criminal, civil or administrative proceeding arising from a violation of or failure to comply with law. In the final rule, we do not include this definition in § 164.512(f), because it is redundant with the definition of ''law enforcement official'' in § 164.501.

Proposed § 164.510(f)(1) of the NPRM would have authorized disclosure of protected health information to a law enforcement official conducting or supervising a law enforcement inquiry or proceeding authorized by law pursuant to process, under three circumstances.

First, we proposed to permit such disclosures pursuant to a warrant, subpoena, or other order issued by a judicial officer that documented a finding by the officer. The NPRM did not specify requirements for the nature of the finding. In the final rule, we eliminate the requirement for a ''finding,'' and we make changes to the list of orders in response to which covered entities may disclose under this provision. Under the final rule, covered entities may disclose protected health information in compliance with and as limited by relevant requirements of: a court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer. We made this change to the list to conform to the definition of ''required by law'' in § 164.501.

Second, we proposed to permit such disclosures pursuant to a state or federal grand jury subpoena. In the final rule, we leave this provision of the NPRM unchanged.

Third, we proposed to permit such disclosures pursuant to an administrative request, including an administrative subpoena or summons, a civil investigative demand, or similar process, under somewhat stricter standards than exist today for such disclosures. We proposed to permit a covered entity to disclose protected health information pursuant to an administrative request only if the request met three conditions, as follows: (i) The information sought was relevant and material to a legitimate law enforcement inquiry; (ii) the request was as specific and narrowly drawn as reasonably practicable; and (iii) de-identified information could not reasonably have been used to meet the purpose of the request.

The final rules generally adopts this provision of the NPRM. In the final rule, we modify the list of orders in response to which covered entities may disclose protected health information, to include administrative subpoenas or summons, civil or authorized investigative demands, or similar process authorized by law. We made this change to the list to conform with the definition of ''required by law'' in § 164.501. In addition, we slightly modify the second of the three conditions under which covered entities may respond to such requests, to allow disclosure if the request is specific and is limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.

Limited Information for Identification and Location Purposes

The NPRM would have allowed covered entities to disclose ''limited identifying information'' for purposes of identifying a suspect, fugitive, material witness, or missing person, in response to a law enforcement request. We proposed to define ''limited identifying information'' as (i) name; (ii) address; (iii) Social Security number; (iv) date of birth; (v) place of birth; (vi) type of injury or other distinguishing characteristic; and (vii) date and time of treatment.

The final rules generally adopts this provision of the NPRM with a few modifications. In the final rule, we expand the circumstances under which limited information about suspects, fugitives, material witnesses, and missing persons may be disclosed, to include not only cases in which law enforcement officials are seeking to identify such individuals, but also cases in which law enforcement officials are seeking to locate such individuals. In addition, the final rule modifies the list of data elements that may be disclosed under this provision, in several ways. We expand the list of elements that may be disclosed under these circumstances, to include ABO blood type and Rh factor, as well as date and time of death, if applicable. We remove ''other distinguishing characteristic'' from the list of items that may be disclosed for the location and identification purposes described in this paragraph, and instead allow covered entities to disclose only a description of distinguishing physical characteristics, such as scars and tattoos, height, weight, gender, race, hair and eye color, and the presence or absence of facial hair such as a beard or moustache. In addition, in the final rule, protected health information associated with the following cannot be disclosed pursuant to § 164.512(f)(2): DNA data and analyses; dental records; or typing, samples or analyses of tissues or bodily fluids other than blood (*e.g.,* saliva). If a covered entity discloses additional information under this provision, the covered entity will be out of compliance and subject to sanction.

We clarify our intent not to allow covered entities to initiate disclosures of limited identifying information to law enforcement in the absence of a law enforcement request; a covered entity may disclose protected health information under this provision only in response to a request from law enforcement. We allow a ''law enforcement official's request'' to be

made orally or in writing, and we intend for it to include requests by a person acting on behalf of law enforcement, for example, requests by a media organization making a television or radio announcement seeking the public's assistance in identifying a suspect. Such a request also may include a ''Wanted'' poster and similar postings.

Disclosure About a Victim of Crime

The NPRM would have allowed covered entities to disclose protected health information about a victim of a crime, abuse or other harm to a law enforcement official, if the law enforcement official represented that: (i) The information was needed to determine whether a violation of law by a person other than the victim had occurred; and (ii) immediate law enforcement activity that depended on obtaining the information may have been necessary.

The final rule modifies the conditions under which covered entities can disclose protected health information about victims. In addition, as discussed above, the final rule includes a new § 164.512(c), which establishes conditions for disclosure of protected health information about victims of abuse, neglect or domestic violence. In addition, as discussed above, we have added § 164.512(f)(1)(i) to this paragraph to explicitly recognize that in some cases, covered entities' disclosure of protected health information is mandated by state or other law. The rule's requirements for disclosure in situations not covered under mandatory reporting laws are different from the rule's provisions regarding disclosure pursuant to a mandatory reporting law.

The final rule requires covered entities to obtain individual agreement as a condition of disclosing the protected health information about victims to law enforcement, unless the disclosure is permitted under § 164.512(b) or (c) or § 164.512(f)(1) above. The required agreement may be obtained orally, and does not need to meet the requirements of § 164.508 of this rule (regarding authorizations). The rule waives the requirement for individual agreement if the victim is unable to agree due to incapacity or other emergency circumstance and: (1) The law enforcement official represents that the protected health information is needed to determine whether a violation of law by a person other than the victim has occurred and the information is not intended to be used against the victim; (2) the law enforcement official represents that immediate law enforcement activity that depends on such disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and (3) the covered entity, in the exercise of professional judgment, determines that the disclosure is in the individual's best interests. We intend that assessing the individual's best interests includes taking into account any further risk of harm to the individual. This provision does not allow covered entities to initiate disclosures of protected health information to law enforcement; the disclosure must be in response to a request from law enforcement.

We do not intend to create a new legal duty on the part of covered entities with respect to the safety of their patients. Rather, we intend to ensure that covered entities can continue to exercise their professional judgment in these circumstances, on a case-by-case basis, as they do today.

In some cases, a victim may also be a fugitive or suspect. For example, an individual may receive a gunshot wound during a robbery and seek treatment in a hospital emergency room. In such cases, when law enforcement officials are requesting protected health information because the individual is a suspect (and thus the information may be used against the individual), covered entities may disclose the protected health information pursuant to § 164.512(f)(2) regarding suspects and not pursuant to § 164.512(f)(3) regarding victims. Thus, in these situations, covered entities may disclose only the limited identifying information listed in § 164.512(f)(2)—not all of the protected health information that may be disclosed under § 164.512(f)(3).

The proposed rule did not address whether a covered entity could disclose protected health information to a law enforcement official to alert the official of the individual's death.

Disclosures About Decedents

In the final rule, we add a new provision § 164.512(f)(4) in which we permit covered entities to disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death if the covered entity has a suspicion that such death may have resulted from criminal conduct. In such circumstances consent of the individual is not available and it may be difficult to determine the identity of a personal representative and gain consent for disclosure of protected health information. Permitting disclosures in this circumstance will permit law enforcement officials to begin their investigation into the death more rapidly, increasingly the likelihood of success.

Intelligence and National Security Activities

Section 164.510(f)(4) of the NPRM would have allowed covered entities to disclose protected health information to a law enforcement official without individual authorization for the conduct of lawful intelligence activities conducted pursuant to the National Security Act of 1947 (50 U.S.C. 401 *et seq.*) or in connection with providing protective services to the President or other individuals pursuant to section 3056 of title 18, United States Code. In the final rule, we move provisions regarding disclosures of protected health information for intelligence and protective services activities to § 164.512(k) regarding uses and disclosures for specialized government functions.

Criminal Conduct on the Premises of a Covered Entity

The NPRM would have allowed covered entities on their own initiative to disclose to law enforcement officials protected health information that the covered entity believed in good faith constituted evidence of criminal conduct that arose out of and was directly related to: (A) The receipt of health care or payment for health care, including a fraudulent claim for health care; (B) qualification for or receipt of benefits, payments, or services based on a fraudulent statement or material misrepresentation of the health of the individual; that occurred on the covered entity's premises or was witnessed by a member of the covered entity's workforce.

In the final rule, we modify this provision substantially, by eliminating language allowing disclosures already permitted in other sections of the regulation. The proposed provision overlapped with other sections of the NPRM, in particular proposed § 164.510(c) regarding disclosure for health oversight activities. In the final regulation, we clarify that this provision applies only to disclosures to law enforcement officials of protected health information that the covered entity believes in good faith constitutes evidence of a crime committed on the premises. We eliminate proposed § 164.510(f)(5)(i) regarding health care fraud from the law enforcement section, because all disclosures that would have been allowed under that provision are allowed under § 164.512(d) of the final rule (health oversight). Similarly, in the final rule, we eliminate proposed

§ 164.510(f)(5)(iii) on disclosure of protected health information to law enforcement officials regarding criminal activity witnessed by a member of a health plan workforce. All disclosures that would have been permitted by that provision are included in § 164.512(f)(5), which allows disclosure of information to report a crime committed on the covered entity's premises, and by § 164.502, which provides that a covered entity is not in violation of the rule when a member of its workforce or person working for a business associate uses or discloses protected health information while acting as a ''whistle blower.'' Thus, § 164.512(f)(5) allows covered entities to disclose health information only on the good faith belief that it constitutes evidence of a crime on their premises. The preamble to the NPRM said that if the covered entity disclosed protected health information in good faith but was wrong in its belief that the information was evidence of a violation of law, the covered entity would not be subject to sanction under this regulation. The final rule retains this approach.

Reporting Crime in Emergencies

The proposed rule did not address disclosures by emergency medical personnel to a law enforcement official intended to alert law enforcement about the commission of a crime. Because the provisions of proposed rule were limited to individually identifiable health information that was reduced to electronic form, many communications that occur between emergency medical personnel and law enforcement officials at the scene of a crime would not have been covered by the proposed provisions.

In the final rule we include a new provision § 164.512(f)(6) that addresses ''911'' calls for emergency medical technicians as well as other emergency health care in response to a medical emergency. The final rule permits a covered health care provider providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, to disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to (1) the commission and nature of a crime, (2) the location of such crime or of the victim(s) of such crime, and (3) the identity, description, and location of the perpetrator of such crime. A disclosure is not permitted under this section if health care provider believes that the medical emergency is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care. In such cases, disclosures to law enforcement would be governed by paragraph (c) of this section.

This added provision recognizes the special role of emergency medical technicians and other providers who respond to medical emergencies. In emergencies, emergency medical personnel often arrive on the scene before or at the same time as police officers, firefighters, and other emergency response personnel. In these cases, providers may be in the best position, and sometimes be the only ones in the position, to alert law enforcement about criminal activity. For instance, providers may be the first persons aware that an individual has been the victim of a battery or an attempted murder. They may also be in the position to report in real time, through use of radio or other mechanism, information that may immediately contribute to the apprehension of a perpetrator of a crime.

We note that disclosure under this provision is at the discretion of the health care provider. Disclosures in some instances may be governed more strictly, such as by applicable ethical standards and state and local laws.

Finally, the NPRM also included a proposed § 164.510(f)(5), which duplicated proposed § 164.510(f)(3). The final rule does not include this duplicate provision.

Additional Considerations

As stated in the NPRM, this paragraph is not intended to limit or preclude a covered entity from asserting any lawful defense or otherwise contesting the nature or scope of the process when the procedural rules governing the proceeding so allow. At the same time, it is not intended to create a basis for appealing to federal court concerning a request by state law enforcement officials. Each covered entity will continue to have available legal procedures applicable in the appropriate jurisdiction to contest such requests where warranted.

As was the case with the NPRM, this rule does not create any new affirmative requirement for disclosure of protected health information. Similarly, this section is not intended to limit a covered entity from disclosing protected health information to law enforcement officials where other sections of the rule permit such disclosure, *e.g.*, as permitted by § 164.512(j) to avert an imminent threat to health or safety, for health oversight activities, to coroners or medical examiners, and in other circumstances permitted by the rule. For additional provisions permitting covered entities to disclose protected health information to law enforcement officials, see § 164.512(j)(1)(i) and (ii).

Under the NPRM and under the final rule, to obtain protected health information, law enforcement officials must comply with whatever other law is applicable. In certain circumstances, while this provision could authorize a covered entity to disclose protected health information to law enforcement officials, there could be additional applicable statutes or rules that further govern the specific disclosure. If the preemption provisions of this regulation do not apply, the covered entity must comply with the requirements or limitations established by such other law, regulation or judicial precedent. See §§ 160.201 through 160.205. For example, if state law permits disclosure only after compulsory process with court review, a provider or payor is not allowed to disclose information to state law enforcement officials unless the officials have complied with that requirement. Similarly, disclosure of substance abuse patient records subject to, 42 U.S.C. 290dd–2, and the implementing regulations, 42 CFR part 2, continue to be governed by those provisions.

In some instances, disclosure of protected health information to law enforcement officials will be compelled by other law, for example, by compulsory judicial process or compulsory reporting laws (such as laws requiring reporting of wounds from violent crimes, suspected child abuse, or suspected theft of controlled substances). As discussed above, disclosure of protected health information under such other mandatory law is permitted under § 164.512(a).

In the responses to comments we clarify that items such as cells and tissues are not protected health information, but that analyses of them is. The same treatment would be given other physical items, such as clothing, weapons, or a bloody knife. We note, however, that while these items are not protected health information and may be disclosed, some communications that could accompany the disclosure will be protected health information under the rule. For example, if a person provides cells to a researcher, and tells the researcher that these are an identified individual's cancer cells, that accompanying statement is protected health information about that individual. Similarly, if a person provides a bullet to law enforcement, and tells law enforcement that the bullet was extracted from an identified

individual, the person has disclosed the fact that the individual was treated for a wound, and the additional statement is a disclosure of protected health information.

To be able to make the additional statement accompanying the provision of the bullet, a covered entity must look to the rule to find a provision under which a disclosure may be made to law enforcement. Section 164.512(f) of the rule addresses disclosures for law enforcement purposes. Under § 164.512(f)(1), the additional statement may be disclosed to a law enforcement official if required by law or with appropriate process. Under § 164.512(f)(2), we permit covered entities to disclose limited identifying information without legal process in response to a request from a law enforcement official for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person. Thus, in the case of bullet described above, the covered entity may, in response to a law enforcement request, provide the extracted bullet and such additional limited identifying information as is permitted under § 164.512(f)(2).

Section 164.512(g)—Uses and Disclosures About Decedents

In the NPRM we proposed to allow covered entities to disclose protected health information without individual authorization to coroners and medical examiners, consistent with applicable law, for identification of a deceased person or to determine cause of death.

In § 164.512(g) of the final rule, we permit covered entities to disclose protected health information to coroners, medical examiners, and funeral directors as part of a new paragraph on disclosures related to death. The final rule retains the NPRM approach regarding disclosure of protected health information to coroners and medical examiners, and it allows the information disclosed to coroners and medical examiners to include identifying information about other persons that may be included in the individual's medical record. Redaction of such names is not required prior to disclosing the individual's record to coroners or medical examiners. Since covered entities may also perform duties of a coroner or medical examiner, where a covered entity is itself a coroner or medical examiner, the final rule permits the covered entity to use protected health information in all cases in which it is permitted to disclose such information for its duties as a coroner or medical examiner.

Section 164.512(g) allows covered entities to disclose protected health information to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to a decedent. For example, the rule allows hospitals to disclose to funeral directors the fact that an individual has donated an organ or tissue, because this information has implications for funeral home staff duties associated with embalming. When necessary for funeral directors to carry out their duties, covered entities may disclose protected health information prior to and in reasonable anticipation of the individual's death.

Whereas the NPRM did not address the issue of disclosure of psychotherapy notes without individual authorization to coroners and medical examiners, the final rule allows such disclosures.

The NPRM did not include in proposed § 164.510(e) language stating that where a covered entity was itself a coroner or medical examiner, it could use protected health information for the purposes of engaging in a coroner's or a medical examiner's activities. The final rule includes such language to address situations such as where a public hospital performs medical examiner functions. In such cases, the hospital's on-staff coroners can use protected health information while conducting post-mortem investigations, and other hospital staff can analyze any information associated with these investigations, for example, as part of the process of determining the cause of the individual's death.

Section 164.512(h)—Uses and Disclosures for Cadaveric Donation of Organs, Eyes, or Tissues

In the NPRM we proposed to include the procurement or banking of blood, sperm, organs, or any other tissue for administration to patients in the definition of ''health care'' (described in proposed § 160.103). The NPRM's proposed approach did not differentiate between situations in which the donor was competent to consent to the donation—for example, when an individual is donating blood, sperm, a kidney, or a liver or lung lobe—and situations in which the donor was deceased, for example, when cadaveric organs and tissues were being donated. We also proposed to allow use and disclosure of protected health information for treatment without consent.

In the final rule, we take a different approach. In § 164.512(h), we permit covered entities to disclose protected health information without individual authorization to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for donation and transplantation. This provision is intended to address situations in which an individual has not previously indicated whether he or she seeks to donate organs, eyes, or tissues (and therefore authorized release of protected health information for this purpose). In such situations, this provision is intended to allow covered entities to initiate contact with organ and tissue donation and transplantation organizations to facilitate transplantation of cadaveric organs, eyes, and tissues.

Disclosures and Uses for Government Health Data Systems

In the NPRM we proposed to permit covered entities to disclose protected health information to a government agency, or to a private entity acting on behalf of a government agency, for inclusion in a government health data system collecting health data for analysis in support of policy, planning, regulatory, or management functions authorized by law. The NPRM stated that when a covered entity was itself a government agency collecting health data for these functions, it could use protected health information in all cases for which it was permitted to disclose such information to government health data systems.

In the final rule, we eliminate the provision that would have allowed covered entities to disclose protected health information to government health data systems without authorization. Thus, under the final rule, covered entities cannot disclose protected health information without authorization to government health data systems—or to private health data systems—unless the disclosure is permissible under another provision of the rule.

Disclosures for Payment Processes

In the NPRM we proposed to permit covered entities to disclose, in connection with routine banking activities or payment by debit, credit, or other payment card, or other payment means, the minimum amount of protected health information necessary to complete a banking or payment activity to financial institutions or to entities acting on behalf of financial institutions to authorize, process, clear, settle, bill, transfer, reconcile, or collect payments for financial institutions.

The preamble to the NPRM clarified the proposed rule's intent regarding disclosure of diagnostic and treatment information along with payment

information to financial institutions. The preamble to the proposed rule said that diagnostic and treatment information never was necessary to process a payment transaction. The preamble said we believed that in most cases, the permitted disclosure would include only: (1) The name and address of the account holder; (2) the name and address of the payor or provider; (3) the amount of the charge for health services; (4) the date on which health services were rendered; (5) the expiration date for the payment mechanism, if applicable; and (6) the individual's signature. The preamble noted that the proposed regulation text did not include an exclusive list of information that could lawfully be disclosed to process payments, and it solicited comments on whether more elements would be needed for banking and payment transactions and on whether including a specific list of protected health information that could be disclosed was an appropriate approach.

The preamble also noted that under section 1179 of HIPAA, certain activities of financial institutions were exempt from this rule, to the extent that these activities constituted authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments for health care or health plan premiums.

In the final rule, we eliminate the NPRM's provision on ''banking and payment processes.'' All disclosures that would have been allowed pursuant to proposed § 164.510(i) are allowed under § 164.502(a) of the final rule, regarding disclosure for payment purposes.

Section 164.512(i)—Uses and Disclosures for Research Purposes

The NPRM would have permitted covered entities to use and disclose protected health information for research—regardless of funding source—without individual authorization, provided that the covered entity obtained documentation of the following:

(1) A waiver, in whole or in part, of authorization for the use or disclosure of protected health information was approved by an Institutional Review Board (IRB) or a privacy board that was composed as stipulated in the proposed rule;

(2) The date of approval of the waiver, in whole or in part, of authorization by an IRB or privacy board;

(3) The IRB or privacy board had determined that the waiver, in whole or in part satisfied the following criteria:

(i) The use or disclosure of protected health information involves no more than minimal risk to the subjects;

(ii) The waiver will not adversely affect the rights and welfare of the subjects;

(iii) The research could not practicably be conducted without the waiver;

(iv) Whenever appropriate, the subjects will be provided with additional pertinent information after participation;

(v) The research could not practicably be conducted without access to and use of the protected health information;

(vi) The research is of sufficient importance so as to outweigh the intrusion of the privacy of the individual whose information is subject to the disclosure;

(vii) There is an adequate plan to protect the identifiers from improper use and disclosure; and

(viii) There is an adequate plan to destroy the identifiers at the earliest opportunity consistent with the conduct of the research, unless there is a health or research justification for retaining the identifiers; and

(4) The written documentation was signed by the chair of, as applicable, the IRB or the privacy board.

The NPRM also proposed that IRBs and privacy boards be permitted to adopt procedures for ''expedited review'' similar to those provided in the Common Rule (Common Rule § .110) for records research that involved no more than minimal risk. However, this provision for expedited review was not included in the proposed regulation text.

The board that would determine whether the research protocol met the eight specified criteria for waiving the patient authorization requirements (described above), could have been an IRB constituted as required by the Common Rule, or a privacy board, whose proposed composition is described below. The NPRM proposed no requirements for the location or sponsorship of the IRB or privacy board. Under the NPRM, the covered entity could have created such a board and could have relied on it to review research proposals for uses and disclosures of protected health information for research. A covered entity also could have relied on the necessary documentation from an outside researcher's own university IRB or privacy board. In addition, a covered entity could have engaged the services of an outside IRB or privacy board to obtain the necessary documentation.

Absent documentation that the requirements described above had been met, the NPRM would have required individuals' authorization for the use or disclosure of protected health information for research, pursuant to the authorization requirements in proposed § 164.508. For research conducted with patient authorization, documentation of IRB or privacy board approval would not have been required.

The final rule retains the NPRM's proposed framework for permitting uses and disclosures of protected health information for research purposes, although we are making several important changes for the final rule. These changes are discussed below:

Documentation Requirements of IRB or Privacy Board Approval of Waiver

The final rule retains these documentation requirements, but modifies some of them and includes two additional documentation requirements. The final rule's modifications to the NPRM's proposed documentation requirements are described first, followed by a description of the three documentation requirements added in the final rule.

The final rule makes the following modifications to the NPRM's proposed documentation requirements for the waiver of individual authorization:

1. *IRB and privacy board membership.* The NPRM stipulated that to meet the requirements of proposed § 164.510(j), the documentation would need to indicate that the IRB had been composed as required by the Common Rule (§ .107), and the privacy board had been composed as follows: ''(A) Has members with varying backgrounds and appropriate professional competency as necessary to review the research protocol; (B) Includes at least one member who is not affiliated with the entity conducting the research, or related to a person who is affiliated with such entity; and (C) Does not have any member participating in a review of any project in which the member has a conflict of interest'' (§ 164.510(j)(1)(ii)).

The final rule modifies the first of the requirements for the composition of a privacy board to focus on the effect of the research protocol on the individual's privacy rights and related interests. Therefore, under the final rule, the required documentation must indicate that the privacy board has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests.

In addition, the final rule further restricts the NPRM's proposed requirement that the privacy board include at least one member who was

not affiliated with the entity conducting the research, or related to a person who is affiliated with such entity. Under the final rule, the board must include at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with such entities.

The other documentation requirements for the composition of an IRB and privacy board remain the same.

2. *Waiver of authorization criteria.* The NPRM proposed to prohibit the use or disclosure of protected health information for research without individual authorization as stipulated in proposed § 164.508 unless the covered entity had documentation indicating that an IRB or privacy board had determined that the following waiver criteria had been met:

(i) The use or disclosure of protected health information involves no more than minimal risk to the subjects;

(ii) The waiver will not adversely affect the rights and welfare of the subjects;

(iii) The research could not practicably be conducted without the waiver;

(iv) Whenever appropriate, the subjects will be provided with additional pertinent information after participation;

(v) The research could not be practicably be conducted without access to and use of the protected health information;

(vi) The research is of sufficient importance so as to outweigh the intrusion of the privacy of the individual whose information is subject to the disclosure;

(vii) There is an adequate plan to protect the identifiers from improper use and disclosure; and

(viii) There is an adequate plan to destroy the identifiers at the earliest opportunity consistent with the conduct of the research, unless there is a health or research justification for retaining the identifiers.

The final rule continues to permit the documentation of IRB or privacy board approval of a waiver of an authorization as required by § 164.508, to indicate that only some or all of the § 164.508 authorization requirements have been waived. In addition, the final rule clarifies that the documentation of IRB or privacy board approval may indicate that the authorization requirements have been altered. Also, for all of the proposed waiver of authorization criteria that used the term ''subject,'' we replace this term with the term ''individual'' in the final rule.

In addition, the final rule (1) eliminates proposed waiver criterion iv, (2) modifies proposed waiver criteria ii, iii, vi, and viii, and (3) adds a waiver criterion.

Proposed waiver criterion ii (waiver criterion § 164.512(i)(2)(ii)(B) in the final rule) is revised as follows to focus more narrowly on the privacy interests of individuals, and to clarify that it also pertains to alterations of individual authorization: ''the alteration or waiver will not adversely affect the privacy rights and the welfare of the individuals.'' Under criterion § 164.512(i)(2)(ii)(B), the question is whether the alteration or waiver of individual authorization would adversely affect the privacy rights and the welfare of individuals, not whether the research project itself would adversely affect the privacy rights or the welfare of individuals.

Proposed waiver criterion iii (waiver criterion § 164.512(i)(2)(ii)(C) in the final rule) is revised as follows to clarify that it also pertains to alterations of individual authorization: ''the research could not practicably be conducted without the alteration or waiver.''

Proposed waiver criterion vi (waiver criterion § 164.512(i)(2)(ii)(E) in the final rule) is revised as follows to be more consistent with one of the Common Rule's requirements for the approval of human subjects research (Common Rule, § .111(a)(2)): ''the privacy risks to individuals whose protected health information is to be used or disclosed are reasonable in relation to anticipated benefits if any to individuals, and the importance of the knowledge that may reasonably be expected to result from the research.'' Under criterion § 164.512(i)(2)(ii)(E), the question is whether the risks to an individual's privacy from participating in the research are reasonable in relation to the anticipated benefits from the research. This criterion is unlike waiver criterion § 164.512(i)(2)(ii)(B) in that it focuses on the privacy risks and benefits of the research project more broadly, not on the waiver of individual authorization.

Proposed waiver criterion viii (waiver criterion § 164.512(i)(2)(ii)(G) in the final rule) is revised as follows: ''there is an adequate plan to destroy the identifiers at the earliest opportunity consistent with the conduct of the research, unless there is a health or research justification for retaining the identifiers, or such retention is otherwise required by law.''

In addition, the final rule includes another waiver criterion: waiver criterion § 164.512(i)(2)(ii)(H). The NPRM proposed no restriction on a researcher's further use or disclosure of protected health information that had been received under proposed § 164.510(j). The final rule requires that the covered entity obtain written agreement from the person or entity receiving protected health information under § 164.512(i) not to re-use or disclose protected health information to any other person or entity, except: (1) As required by law, (2) for authorized oversight of the research project, or (3) for other research for which the use or disclosure of protected health information would be permitted by this subpart. For instance, in assessing whether this criterion has been met, we encourage IRBs and privacy boards to obtain adequate assurances that the protected health information will not be disclosed to an individual's employer for employment decisions without the individual's authorization.

3. *Required signature.* The rule broadens the types of individuals who are permitted to sign the required documentation of IRB or privacy board approval. The final rule requires the documentation of the alteration or waiver of authorization to be signed by (1) the chair of, as applicable, the IRB or the privacy board, or (2) a member of the IRB or privacy board, as applicable, who is designated by the chair to sign the documentation.

Furthermore, the final rule makes the following three additions to the proposed documentation requirements for the alteration or waiver of authorization:

1. *Identification of the IRB or privacy board.* The NPRM did not propose that the documentation of waiver include a statement identifying the IRB or privacy board that approved the waiver of authorization. In the final rule we require that such a statement be included in the documentation of alteration or waiver of individual authorization. By this requirement we mean that the name of the IRB or privacy board must be included in such documentation, not the names of individual members of the board.

2. *Description of protected health information approved for use or disclosure.* The NPRM did not propose that the documentation of waiver include a description of the protected health information that the IRB or privacy board had approved for use or disclosure without individual authorization. In considering waiver of authorization criterion § 164.512(i)(2)(ii)(D), we expect the IRB or privacy board to consider the amount of information that is minimally needed for the study. The final rule requires that the documentation of IRB or

privacy board approval of the alteration or waiver of authorization describe the protected health information for which use or access has been determined to be necessary for the research by the IRB or privacy board. For example, if the IRB or privacy board approves only the use or disclosure of certain information from patients' medical records, and not patients' entire medical record, this must be stated on the document certifying IRB or privacy board approval.

3. *Review and approval procedures.* The NPRM would not have required documentation of IRBs' or privacy boards' review and approval procedures. In the final rule, the documentation of the alteration or waiver of authorization must state that the alteration or waiver has been reviewed and approved by: (1) an IRB that has followed the voting requirements stipulated in the Common Rule (§ .108(b)), or the expedited review procedures as stipulated in § .110(b); or (2) a privacy board that has reviewed the proposed research at convened meetings at which a majority of the privacy board members are present, including at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any such entities, and the alteration or waiver of authorization is approved by the majority of privacy board members present at the meeting, unless an expedited review procedure is used.

For documentation of IRB approval that used an expedited review procedure, the covered entity must ensure that the documentation indicates that the IRB followed the expedited review requirements of the Common Rule (§ .110). For documentation of privacy board approval that used an expedited review procedure, the covered entity must ensure that the documentation indicates that the privacy board met the expedited review requirements of the privacy rule. In the final rule, a privacy board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the protected health information for which disclosure is being sought. If a privacy board elects to use an expedited review procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the privacy board, or by one or more members of the privacy board as designated by the chair. Use of the expedited review mechanism permits review by a single member of the IRB or privacy board, but continues to require that the covered entity obtain documentation that all of the specified waiver criteria have been met.

Reviews Preparatory to Research

Under the NPRM, if a covered entity used or disclosed protected health information for research, but the researcher did not record the protected health information in a manner that persons could be identified, such an activity would have constituted a research use or disclosure that would have been subject to either the individual authorization requirements of proposed § 164.508 or the documentation of the waiver of authorization requirements of proposed § 164.510(j).

The final rule permits the use and disclosure of protected health information for research without requiring authorization or documentation of the alteration or waiver of authorization, if the research is conducted in such a manner that only de-identified protected health information is recorded by the researchers and the protected health information is not removed from the premises of the covered entity. For such uses and disclosures of protected health information, the final rule requires that the covered entity obtain from the researcher representations that use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research, no protected health information is to be removed from the covered entity by the researcher in the course of the review, and the protected health information for which use or access is sought is necessary for the research purposes. The intent of this provision is to permit covered entities to use and disclose protected health information to assist in the development of a research hypothesis and aid in the recruitment of research participants. We understand that researchers sometimes require access to protected health information to develop a research protocol, and to determine whether a specific covered entity has protected health information of prospective research participants that would meet the eligibility criteria for enrollment into a research study. Therefore, this provision permits covered entities to use and disclose protected health information for these preliminary research activities without individual authorization and without documentation that an IRB or privacy board has altered or waived individual authorization.

Research on Protected Health Information of the Deceased

The NPRM would have permitted the use and disclosure of protected health information of deceased persons for research without the authorization of a legal representative, and without the requirement for written documentation of IRB or privacy board approval in proposed § 164.510(j). In the final rule, we retain the exception for uses and disclosures for research purposes but in addition require that the covered entity take certain protective measures prior to release of the decedent's protected health information for such purposes. Specifically, the final rule requires that the covered entity obtain representation that the use or disclosure is sought solely for research on the protected health information of decedent, and representation that the protected health information for which use or disclosure is sought is necessary for the research purposes. In addition, the final rule allows covered entities to request from the researcher documentation of the death of the individuals about whom protected health information is being sought.

Good Faith Reliance

The final rule clarifies that covered entities are allowed to rely on the IRB's or privacy board's representation that the research proposal meets the documentation requirements of § 164.512(i)(1)(i) and the minimum necessary requirements of § 164.514.

In addition, when using or disclosing protected health information for reviews preparatory to research (§ 164.512(i)(1)(ii)) or for research solely on the protected health information of decedents (§ 164.512)(1)(iii)), the final rule clarifies that the covered entity may rely on the requesting researcher's representation that the purpose of the request is for one of these two purpose, and that the request meets the minimum necessary requirements of § 164.514. Therefore, the covered entity has not violated the rule if the requesting researcher misrepresents his or her intended use of the protected health information to the covered entity.

Additional Research Provisions

Research Including Treatment

To the extent that a researcher provided treatment to persons as part of a research study, the NPRM would have covered such researchers as health care providers for purposes of that treatment, and required that the researcher comply with all of the provisions of the rule that

would be applicable to health care providers. The final rule retains this requirement.

Individual Access to Research Information

Under proposed § 164.514, the NPRM would have applied the proposed provision regarding individuals' access to records to research that includes the delivery of treatment. The NPRM proposed an exception to individuals' right to access protected health information for clinical trials, where (1) protected health information was obtained by a covered entity in the course of clinical trial, (2) the individual agreed to the denial of access when consenting to participate in the trial (if the individual's consent to participate was obtained), and (3) the trial was still in progress.

Section 164.524 of the final rule retains this exception to access for research that includes treatment. In addition, the final rule requires that participants in such research be informed that their right of access to protected health information about them will be reinstated once the research is complete.

Obtaining the Individual's Authorization for Research

The NPRM would have required covered entities obtaining individuals' authorization for the use or disclosure of information for research to comply with the requirements applicable to individual authorization for the release of protected health information (proposed § 164.508(a)(2)). If an individual had initiated the use or disclosure of his/her protected health information for research, or any other purpose, the covered entity would have been required to obtain a completed authorization for the use or disclosure of protected health information as proposed in § 164.508(c).

The final rule retains these requirements for research conducted with authorization, as required by § 164.508. In addition, for the use and disclosure of protected health information created by a covered entity for the purpose, in whole or in part, of research that includes treatment of the individual, the covered entity must meet the requirements of § 164.508(f).

Interaction with the Common Rule

The NPRM stated that the proposed rule would not override the Common Rule. Where both the NPRM and the Common Rule would have applied to research conducted by the covered entity—either with or without individuals' authorization—both sets of regulations would have needed to be followed. This statement remains true in the final rule. In addition, we clarify that FDA's human subjects regulations must also be followed if applicable.

Section 164.512(j)—Uses and Disclosures to Avert a Serious Threat to Health or Safety

In the NPRM we proposed to allow covered entities to use or disclose protected health information without individual authorization—consistent with applicable law and ethics standards—based on a reasonable belief that use or disclosure of the protected health information was necessary to prevent or lessen a serious and imminent threat to health or safety of an individual or of the public. Pursuant to the NPRM, covered entities could have used or disclosed protected health information in these emergency circumstances to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat. The NPRM stated that covered entities that made disclosures in these circumstances were presumed to have acted under a reasonable belief if the disclosure was made in good faith, based on credible representation by a person with apparent knowledge or authority. The NPRM did not include verification requirements specific to this paragraph.

In § 164.512(j) of the final rule, we retain the NPRM's approach to uses and disclosures made to prevent or lessen serious and imminent threats to health or safety, as well as its language regarding the presumption of good faith. We also clarify that: (1) Rules governing these situations, which the NPRM referred to as ''emergency circumstances,'' are not intended to apply to emergency care treatment, such as health care delivery in a hospital emergency room; and (2) the ''presumption of good faith belief'' is intended to apply only to this provision and not to all disclosures permitted without individual authorization. The final rule allows covered entities to use or disclose protected health information without an authorization on their own initiative in these circumstances, when necessary to prevent or lessen a serious and imminent threat, consistent with other applicable ethical or legal standards.

The rule's approach is consistent with the ''duty to warn'' third persons at risk, which has been established through case law. In *Tarasoff* v. *Regents of the University of California* (17 Cal. 3d 425 (1976)), the Supreme Court of California found that when a therapist's patient had made credible threats against the physical safety of a specific person, the therapist had an obligation to use reasonable care to protect the intended victim of his patient against danger, including warning the victim of the danger. Many states have adopted, through either statutory or case law, versions of the Tarasoff duty to warn. The rule is not intended to create a duty to warn or disclose. Rather, it permits disclosure to avert a serious and imminent threat to health or safety consistent with other applicable legal or ethical standards. If disclosure in these circumstances is prohibited by state law, this rule would not allow the disclosure.

As indicated above, in some situations (for example, when a person is both a fugitive and a victim and thus covered entities could disclose protected health information pursuant either to § 164.512(f)(2) regarding fugitives or to § 164.512(f)(3) establishing conditions for disclosure about victims), more than one section of this rule potentially could apply with respect to a covered entity's potential disclosure of protected health information. Similarly, in situations involving a serious and imminent threat to public health or safety, law enforcement officials may be seeking protected health information from covered entities to locate a fugitive. In the final rule, we clarify that if a situation fits one section of the rule (for example, § 164.512(j) on serious and imminent threats to health or safety), covered entities may disclose protected health information pursuant to that section, regardless of whether the disclosure also could be made pursuant to another section (*e.g.,* § 164.512(f)), regarding disclosure to law enforcement officials).

The proposed rule did not address situations in which covered entities could make disclosures to law enforcement officials about oral statements admitting participation in violent conduct or about escapees.

In the final rule we permit, but do not require, covered entities to use or disclose protected health information, consistent with applicable law and standards of ethical conduct, in specific situations in which the covered entity, in good faith, believes the use or disclosure is necessary to permit law enforcement authorities to identify or apprehend an individual. Under paragraph (j)(1)(ii)(A) of this section, a covered entity may take such action because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have resulted in serious physical harm to the victim. The

protected health information that is disclosed in this case is limited to the statement and to the protected health information included under the limited identifying and location information in § 164.512(f)(2), such as name, address, and type of injury. Under paragraph (j)(1)(ii)(B) of this section, a covered entity may take such action where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody.

A disclosure may not be made under paragraph (j)(1)(ii)(A) for a statement admitting participation in a violent crime if the covered entity learns the information in the course of counseling or therapy. Similarly, such a disclosure is not permitted if the covered entity learns the information in the course of treatment to affect the propensity to commit the violent crimes that are described in the individual's statements. We do not intend to discourage individuals from speaking accurately in the course of counseling or therapy sessions, or to discourage other treatment that specifically seeks to reduce the likelihood that someone who has acted violently in the past will do so again in the future. This prohibition on disclosure is triggered once an individual has made a request to initiate or be referred to such treatment, therapy, or counseling.

The provision permitting use and disclosure has been added in light of the broadened definition in the final rule of protected health information. Under the NPRM, protected health information meant individually identifiable health information that is or has been electronically transmitted or electronically maintained by a covered entity. Under the final rule, protected health information includes information transmitted by electronic media as well as such information transmitted or maintained in any other form or medium. The new definition includes oral statements to covered entities as well as individually identifiable health information transmitted ''in any other form.''

The definition of protected health information, for instance, would now apply to a statement by a patient that is overheard by a hospital security guard in a waiting room. Such a statement would have been outside the scope of the proposed rule (unless it was memorialized in an electronic record), but is within the scope of the final rule. For the example with the hospital guard, the new provision permitting disclosure of a statement by an individual admitting participation in a violent crime would have the same effect as the proposed rule—the statement could be disclosed to law enforcement, so long as the other aspects of the regulation are followed. Similarly, where it appears from all the circumstances that the individual has escaped from prison, the expanded definition of protected health information should not prevent the covered entity from deciding to report this information to law enforcement.

The disclosures that covered entities may elect to make under this paragraph are entirely at their discretion. These disclosures to law enforcement are in addition to other disclosure provisions in the rule. For example, under paragraph § 164.512(f)(2) of this section, a covered entity may disclose limited categories of protected health information in response to a request from a law enforcement official for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person. Paragraph § 164.512(f)(1) of this section permits a covered entity to make disclosures that are required by other laws, such as state mandatory reporting laws, or are required by legal process such as court orders or grand jury subpoena.

Section 164.512(k)—Uses and Disclosures for Specialized Government Functions

Application to Military Services

In the NPRM we would have permitted a covered entity providing health care to Armed Forces personnel to use and disclose protected health information for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, where the appropriate military authority had published by notice in the **Federal Register** (In the NPRM, we proposed that the Department of Defense would publish this **Federal Register** notice in the future.) The final rule takes a similar approach while making some modifications to the NPRM. One modification concerns the information that will be required in the **Federal Register** notice. The NPRM would have required a listing of (i) appropriate military command authorities; (ii) the circumstances for which use or disclosure without individual authorization would be required; and (iii) activities for which such use or disclosure would occur in order to assure proper execution of the military mission. In the final rule, we eliminate the third category and also slightly modify language in the second category to read: ''the purposes for which the protected health information may be used or disclosed.''

An additional modification concerns the rule's application to foreign military and diplomatic personnel. The NPRM would have excluded foreign diplomatic and military personnel, as well as their dependents, from the proposed definition of ''individual,'' thereby excluding any protected health information created about these personnel from the NPRM's privacy protections. Foreign military and diplomatic personnel affected by this provision include, for example, allied military personnel who are in the United States for training. The final rule applies a more limited exemption to foreign military personnel only (Foreign diplomatic personnel will have the same protections granted to all other individuals under the rule). Under the final rule, foreign military personnel are not excluded from the definition of ''individual.'' Covered entities will be able to use and disclose protected health information of foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for U.S. Armed Forces personnel under the notice to be published in the **Federal Register**. Foreign military personnel do have the same rights of access, notice, right to request privacy protection, copying, amendment, and accounting as do other individuals pursuant to §§ 164.520–164.526 (sections on access, notice, right to request privacy protection for protected health information, amendment, inspection, copying) of the rule.

The NPRM likewise would have exempted overseas foreign national beneficiaries from the proposed rule's requirements by excluding them from the definition of ''individual.'' Under the final rule, these beneficiaries no longer are exempt from the definition of ''individual.'' However, the rule's provisions do not apply to the individually identifiable health information of overseas foreign nationals who receive care provided by the Department of Defense, other federal agencies, or by non-governmental organizations incident to U.S. sponsored missions or operations.

The final rule includes a new provision to address separation or discharge from military service. The preamble to the NPRM noted that upon completion of individuals' military service, DOD and the Department of Transportation routinely transfer entire military service records, including protected health information to the Department of Veterans Affairs so that

the file can be retrieved quickly if the individuals or their dependents apply for veterans benefits. The NPRM would have required consent for such transfers. The final rule no longer requires consent in such situations. Thus, under the final rule, a covered entity that is a component of DOD or the Department of Transportation may disclose to DVA the protected health information of an Armed Forces member upon separation or discharge from military service for the purpose of a determination by DVA of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs.

Department of Veterans Affairs

Under the NPRM, a covered entity that is a component of the Department of Veterans Affairs could have used and disclosed protected health information to other components of the Department that determine eligibility for, or entitlement to, or that provide benefits under the laws administered by the Secretary of Veterans Affairs. In the final rule, we retain this approach.

Application to Intelligence Community

The NPRM would have provided an exemption from its proposed requirements to the intelligence community. As defined in section 4 of the National Security Act, 50 U.S.C. 401a, the intelligence community includes: the Office of the Director of Central Intelligence Agency; the Office of the Deputy Director of Central Intelligence; the National Intelligence Council and other such offices as the Director may designate; the Central Intelligence Agency; the National Security Agency; the Defense Intelligence Agency; the National Imagery and Mapping Agency ; the National Reconnaissance Office; other offices within the DOD for the collection of specialized national intelligence through reconnaissance programs; the intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Federal Bureau of Investigation, the Department of the Treasury, and the Department of Energy; the Bureau of Intelligence and Research of the Department of State; and such other elements of any other department or agency as may be designated by the President, or designated jointly by the Director of Central Intelligence and the head of the department or agency concerned, as an element of the intelligence community. It would have allowed a covered entity to use without individual authorization protected health information of employees of the intelligence community, and of their dependents, if such dependents were being considered for posting abroad. The final rule does not include such an exemption. Rather, the final rule does not except intelligence community employees and their dependents from the general rule requiring an authorization in order for protected health information to be used and disclosed.

National Security and Intelligence Activities

The NPRM included a provision, in § 164.510(f)—Disclosure for Law Enforcement Purposes—that would allow covered entities to disclose protected health information without consent for the conduct of lawful intelligence activities under the National Security Act, and in connection with providing protective services to the President or to foreign heads of state pursuant to 18 U.S.C. 3056 and 22 U.S.C. 2709(a)(3) respectively. The final rule preserves these exemptions, with slight modifications, but moves them from proposed § 164.510(f) to § 164.512(k). It also divides this area into two paragraphs—one called ''National Security and Intelligence Activities'' and the second called ''Protective services for the President and Others.''

The final rule, with modifications, allows a covered entity to disclose protected health information to an authorized federal official for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act and implementing authority (*e.g.,* Executive Order 1233). The references to ''counter-intelligence and other national security activities'' are new to the final rule. The reference to ''implementing authority (*e.g.* Executive Order 12333)'' is also new. The final rule also adds specificity to the provision on protective services. It states that a covered entity may disclose protected health information to authorized federal officials for the provision of protective services to the President or other persons as authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons as authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879.

Application to the State Department

The final rule creates a narrower exemption for Department of State for uses and disclosures of protected health information (1) for purposes of a required security clearance conducted pursuant to Executive Orders 10450 and 12698; (2) as necessary to meet the requirements of determining worldwide availability or availability for mandatory service abroad under Sections 101(a)(4) and 504 of the Foreign Service Act; and (3) for a family member to accompany a Foreign Service Officer abroad, consistent with Section 101(b)(5) and 904 of the Foreign Service Act.

Regarding security clearances, nothing prevents any employer from requiring that individuals provide authorization for the purpose of obtaining a security clearance. For the Department of State, however, the final rule provides a limited exemption that allows a component of the Department of State without an authorization to (1) use protected health information to make medical suitability determinations and (2) to disclose whether or not the individual was determined to be medically suitable to authorized officials in the Department of State for the purpose of a security clearance investigation conducted pursuant to Executive Order 10450 and 12698.

Sections 101(a)(4) and 504 of the Foreign Service Act require that Foreign Service members be available to serve in assignments throughout the world. The final rule permits disclosures to officials who need protected health information to determine availability for duty worldwide.

Section 101(b)(5) of the Foreign Service Act requires the Department of State to mitigate the impact of hardships, disruptions, and other unusual conditions on families of Foreign Service Officers. Section 904 requires the Department to establish a health care program to promote and maintain the physical and mental health of Foreign Service member family members. The final rule permits disclosure of protected health information to officials who need protected health information for a family member to accompany a Foreign Service member abroad.

This exemption does not permit the disclosure of specific medical conditions, diagnoses, or other specific medical information. It permits only the disclosure of the limited information needed to determine whether the individual should be granted a security clearance or whether the Foreign Service member of his or her family members should be posted to a certain overseas assignment.

Application to Correctional Facilities

The NPRM would have excluded the individually identifiable health information of correctional facility inmates and detention facility detainees from the definition of protected health information. Thus, none of the NPRM's

proposed privacy protections would have applied to correctional facility inmates or to detention facility detainees while they were in these facilities or after they had been released.

The final rule takes a different approach. First, to clarify that we are referring to individuals who are incarcerated in correctional facilities that are part of the criminal justice system or in the lawful custody of a law enforcement official—and not to individuals who are ''detained'' for non-criminal reasons, for example, in psychiatric institutions—§ 164.512(k) covers disclosure of protected health information to correctional institutions or law enforcement officials having such lawful custody. In addition, where a covered health care provider is also a health care component of a correctional institution, the final rule permits the covered entity to use protected health information in all cases in which it is permitted to disclose such information.

We define correctional institution as defined pursuant to 42 U.S.C. 13725(b)(1), as a ''prison, jail, reformatory, work farm, detention center, or halfway house, or any other similar institution designed for the confinement or rehabilitation of criminal offenders.'' The rules regarding disclosure and use of protected health information specified in § 164.512(k) cover individuals who are in transitional homes, and other facilities in which they are required by law to remain for correctional reasons and from which they are not allowed to leave. This section also covers individuals who are confined to psychiatric institutions for correctional reasons and who are not allowed to leave; however, it does not apply to disclosure of information about individuals in psychiatric institutions for treatment purposes only, who are not there due to a crime or under a mandate from the criminal justice system. The disclosure rules described in this section do not cover release of protected health information about individuals in pretrial release, probation, or on parole, such persons are not considered to be incarcerated in a correctional facility.

As described in § 164.512(k), correctional facility inmates' individually identifiable health information is not excluded from the definition of protected health information. When individuals are released from correctional facilities, they will have the same privacy rights that apply to all other individuals under this rule.

Section 164.512(k) of the final rule states that while individuals are in a correctional facility or in the lawful custody of a law enforcement official, covered entities (for example, the prison's clinic) can use or disclose protected health information about these individuals without authorization to the correctional facility or the law enforcement official having custody as necessary for: (1) The provision of health care to such individuals; (2) the health and safety of such individual or other inmates; (3) the health and safety of the officers of employees of or others at the correctional institution; and (4) the health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution or facility to another; (5) law enforcement on the premises of the correctional institution; and (6) the administration and maintenance of the safety, security, and good order of the correctional institution. This section is intended to allow, for example, a prison's doctor to disclose to a van driver transporting a criminal that the individual is a diabetic and frequently has seizures, as well as information about the appropriate action to take if the individual has a seizure while he or she is being transported.

We permit covered entities to disclose protected health information about these individuals if the correctional institution or law enforcement official represents that the protected health information is necessary for these purposes. Under 164.514(h), a covered entity may reasonably rely on the representation of such public officials.

Application to Public Benefits Programs Required to Share Eligibility Information

We create a new provision for covered entities that are a government program providing public benefits. This provision allows the following disclosures of protected health information.

First, where other law requires or expressly authorizes information relating to the eligibility for, or enrollment in more than one public program to be shared among such public programs and/or maintained in a single or combined data system, a public agency that is administering a health plan may maintain such a data base and may disclose information relating to such eligibility or enrollment in the health plan to the extent authorized by such other law.

Where another public entity has determined that the appropriate balance between the need for efficient administration of public programs and public funds and individuals' privacy interests is to allow information sharing for these limited purposes, we do not upset that determination. For example, section 1137 of the Social Security Act requires a variety of public programs, including the Social Security program, state medicaid programs, the food stamp program, certain unemployment compensation programs, and others, to participate in a joint income and eligibility verification system. Similarly, section 222 of the Social Security Act requires the Social Security Administration to provide information to certain state vocational rehabilitation programs for eligibility purposes. In some instances, it is a covered entity that first collects or creates the information that is then disclosed for these systems. We do not prohibit those disclosures.

This does not authorize these entities to share information for claims determinations or ongoing administration of these public programs. This provision is limited to the agencies and activities described above.

Second, § 164.512(k)(6) permits a covered entity that is a government agency administering a government program providing public benefits to disclose protected health information relating to the program to another covered entity that is a government agency administering a government program providing public benefits if the programs serve the same or similar populations and the disclosure of protected health information is necessary to coordinate the covered functions of such programs.

The second provision permits covered entities that are government program providing public benefits that serve the same or similar populations to share protected health information for the purposes of coordinating covered functions of the programs and for general management and administration relating to the covered functions of the programs. Often, similar government health programs are administered by different government agencies. For example, in some states, the Medicaid program and the State Children's Health Insurance Program are administered by different agencies, although they serve similar populations. Many states coordinate eligibility for these two programs, and sometimes offer services through the same delivery systems and contracts. This provision would permit the covered entities administering these programs to share protected health information of program participants to coordinate enrollment and services and to generally improve the health care operations of the programs. We note that this provision does not authorize the

agencies to use or disclose the protected health information that is shared for purposes other than as provided for in this paragraph.

Section 164.512(l)—Disclosures For Workers' Compensation

The NPRM did not contain special provisions permitting covered entities to disclose protected health information for the purpose of complying with workers' compensation and similar laws. Under HIPAA, workers' compensation and certain other forms of insurance (such as automobile or disability insurance) are ''excepted benefits.'' Insurance carriers that provide this coverage are not covered entities even though they provide coverage for health care services. To carry out their insurance functions, these non-covered insurers typically seek individually identifiable health information from covered health care providers and group health plans. In drafting the proposed rule, the Secretary was faced with the challenge of trying to carry out the statutory mandate of safeguarding the privacy of individually identifiable health information by regulating the flow of such information from covered entities while at the same time respecting the Congressional intent to shield workers' compensation carriers and other excepted benefit plans from regulation as covered entities.

In the proposed rule we allowed covered entities to disclose protected health information without individual consent for purposes of treatment, payment or health care operations—even when the disclosure was to a non-covered entity such as a workers' compensation carrier. In addition, we allowed protected health information to be disclosed if required by state law for purposes of determining eligibility for coverage or fitness for duty. The proposed rule also required that whenever a covered entity disclosed protected health information to a non-covered entity, even though authorized under the rule, the individual who was the subject of the information must be informed that the protected health information was no longer subject to privacy protections.

Like other disclosures under the proposed rule, the information provided to workers' compensation carriers for treatment, payment or health care operations was subject to the minimum necessary standard. However, to the extent that protected health information was disclosed to the carrier because it was required by law, it was not subject to the minimum necessary standard. In addition, individuals were entitled to an accounting when protected health information was disclosed for purposes other than treatment, payment or health care operations.

In the final rule, we include a new provision in this section that clarifies the ability of covered entities to disclose protected health information without authorization to comply with workers' compensation and similar programs established by law that provide benefits for work-related illnesses or injuries without regard to fault. Although most disclosures for workers' compensation would be permissible under other provisions of this rule, particularly the provisions that permit disclosures for payment and as required by law, we are aware of the significant variability among workers' compensation and similar laws, and include this provision to ensure that existing workers' compensation systems are not disrupted by this rule. We note that the minimum necessary standard applies to disclosures under this paragraph.

Under this provision, a covered entity may disclose protected health information regarding an individual to a party responsible for payment of workers' compensation benefits to the individual, and to an agency responsible for administering and/or adjudicating the individual's claim for workers' compensation benefits. For purposes of this paragraph, workers' compensation benefits include benefits under programs such as the Black Lung Benefits Act, the federal Employees' Compensation Act, the Longshore and Harbor Workers' Compensation Act, and the Energy Employees' Occupational Illness Compensation Program Act.

Additional Considerations

We have included a general authorization for disclosures under workers' compensation systems to be consistent with the intent of Congress, which defined workers' compensation carriers as excepted benefits under HIPAA. We recognize that there are significant privacy issues raised by how individually identifiable health information is used and disclosed in workers' compensation systems, and believe that states or the federal government should enact standards that address those concerns.

Section 164.514—Other Procedural Requirements Relating To Uses and Disclosures of Protected Health Information

Section 164.514(a)–(c)—De-identification

In § 164.506(d) of the NPRM, we proposed that the privacy standards would apply to ''individually identifiable health information,'' and not to information that does not identify the subject individual. The statute defines individually identifiable health information as certain health information:

(i) Which identifies the individual, or

(ii) With respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

As we pointed out in the NPRM, difficulties arise because, even after removing obvious identifiers (*e.g.,* name, social security number, address), there is always some probability or risk that any information about an individual can be attributed to that individual.

The NPRM proposed two alternative methods for determining when sufficient identifying information has been removed from a record to render the information de-identified and thus not subject to the rule. First, the NPRM proposed the establishment of a ''safe harbor'': if all of a list of 19 specified items of information had been removed, and the covered entity had no reason to believe that the remaining information could be used to identify the subject of the information (alone or in combination with other information), the covered entity would have been presumed to have created de-identified information. Second, the NPRM proposed an alternative method so that covered entities with sufficient statistical experience and expertise could remove or encrypt a combination of information different from the enumerated list, using commonly accepted scientific and statistical standards for disclosure avoidance. Such covered entities would have been able to include information from the enumerated list of 19 items if they (1) believed that the probability of re-identification was very low, and (2) removed additional information if they had a reasonable basis to believe that the resulting information could be used to re-identify someone.

We proposed that covered entities and their business partners be permitted to use protected health information to create de-identified health information using either of these two methods. Covered entities would have been permitted to further use and disclose such de-identified information in any way, provided that they did not disclose the key or other mechanism that would have enabled the information to be re-identified, and provided that they reasonably believed that such use or disclosure of de-identified information would not have resulted in the use or

disclosure of protected health information.

A number of examples were provided of how valuable such de-identified information would be for various purposes. We expressed the hope that covered entities, their business partners, and others would make greater use of de-identified health information than they do today, when it is sufficient for the purpose, and that such practice would reduce the burden and the confidentiality concerns that result from the use of individually identifiable health information for some of these purposes.

In §§ 164.514(a)-(c) of this final rule, we make several modifications to the provisions for de-identification. First, we explicitly adopt the statutory standard as the basic regulatory standard for whether health information is individually identifiable health information under this rule. Information is not individually identifiable under this rule if it does not identify the individual, or if the covered entity has no reasonable basis to believe it can be used to identify the individual. Second, in the implementation specifications we reformulate the two ways in which a covered entity can demonstrate that it has met the standard.

One way a covered entity may demonstrate that it has met the standard is if a person with appropriate knowledge and experience applying generally accepted statistical and scientific principles and methods for rendering information not individually identifiable makes a determination that the risk is very small that the information could be used, either by itself or in combination with other available information, by anticipated recipients to identify a subject of the information. The covered entity must also document the analysis and results that justify the determination. We provide guidance regarding this standard in our responses to the comments we received on this provision.

We also include an alternate, safe harbor, method by which covered entities can demonstrate compliance with the standard. Under the safe harbor, a covered entity is considered to have met the standard if it has removed all of a list of enumerated identifiers, and if the covered entity has no actual knowledge that the information could be used alone or in combination to identify a subject of the information. We note that in the NPRM, we had proposed that to meet the safe harbor, a covered entity must have ''no reason to believe'' that the information remained identifiable after the enumerated identifiers were removed. In the final rule, we have changed the standard to one of actual knowledge in order to provide greater certainty to covered entities using the safe harbor approach.

In the safe harbor, we explicitly allow age and some geographic location information to be included in the de-identified information, but all dates directly related to the subject of the information must be removed or limited to the year, and zip codes must be removed or aggregated (in the form of most 3-digit zip codes) to include at least 20,000 people. Extreme ages of 90 and over must be aggregated to a category of 90+ to avoid identification of very old individuals. Other demographic information, such as gender, race, ethnicity, and marital status are not included in the list of identifiers that must be removed.

The intent of the safe harbor is to provide a means to produce some de-identified information that could be used for many purposes with a very small risk of privacy violation. The safe harbor is intended to involve a minimum of burden and convey a maximum of certainty that the rules have been met by interpreting the statutory ''reasonable basis to believe that the information can be used to identify the individual'' to produce an easily followed, cook book approach.

Covered entities may use codes and similar means of marking records so that they may be linked or later re-identified, if the code does not contain information about the subject of the information (for example, the code may not be a derivative of the individual's social security number), and if the covered entity does not use or disclose the code for any other purpose. The covered entity is also prohibited from disclosing the mechanism for re-identification, such as tables, algorithms, or other tools that could be used to link the code with the subject of the information.

Language to clarify that covered entities may contract with business associates to perform the de-identification has been added to the section on business associates.

Section 164.514(d)—Minimum Necessary

The proposed rule required a covered entity to make all reasonable efforts not to use or disclose more than the minimum amount of protected health information necessary to accomplish the intended purpose of the use or disclosure (proposed § 164.506(b)).

The proposed minimum necessary standard did not apply to uses or disclosures that were made by covered entities at the request of the individual, either to allow the individual access to protected health information about him or her or pursuant to an authorization initiated by the individual. The requirement also did not apply to uses and disclosures made: pursuant to the compliance and enforcement provisions of the rule; as required by law and permitted by the regulation without individual authorization; by a covered health care provider to a health plan, when the information was requested for audit and related purposes. Finally, the standard did not apply to the HIPAA administrative simplification transactions.

The proposed implementation specifications would have required a covered entity to have procedures to: (i) Identify appropriate persons within the entity to determine what information should be used or disclosed consistent with the minimum necessary standard; (ii) ensure that those persons make the minimum necessary determinations, when required; and (iii) within the limits of the entity's technological capabilities, provide for the making of such determinations individually. The proposal allowed a covered entity, when making disclosures to public officials that were permitted without individual authorization but not required by other law, to reasonably rely on the representations of such officials that the information requested was the minimum necessary for the stated purpose(s).

The preamble provided further guidance. The preamble explained that covered entities could not have general policies of approving all requests (or all requests of a particular type) without carefully considering certain criteria (see ''Criteria,'' below) as well as other information specific to the request. The minimum necessary determination would have needed to be consistent with and directly related to the purpose of the use or disclosure. Where there was ambiguity regarding the information to be used or disclosed, the preamble directed covered entities to interpret the ''minimum necessary'' standard to ''require'' the covered entity to make some effort to limit the amount of protected health information used/disclosed.

The proposal would have required the minimum necessary determination to take into consideration the ability of a covered entity to delimit the amount of information used or disclosed. The preamble noted that these determinations would have to be made under a reasonableness standard: covered entities would be required to make reasonable efforts and to incur reasonable expense to limit the use or

disclosure. The ''reasonableness'' of limiting particular uses or disclosures was to be determined based on the following factors (which were not included in the regulatory text):

a. The extent to which the use or disclosure would extend the number of persons with access to the protected health information.

b. The likelihood that further uses or disclosures of the protected health information could occur.

c. The amount of protected health information that would be used or disclosed.

d. The importance of the use or disclosure.

e. The potential to achieve substantially the same purpose with de-identified information. For disclosures, each covered entity would have been required to have policies for determining when protected health information must be stripped of identifiers.

f. The technology available to limit the amount of protected health information used/disclosed.

g. The cost of limiting the use/disclosure.

h. Any other factors that the covered entity believed were relevant to the determination.

The proposal shifted the ''minimum necessary'' burden off of covered providers when they were being audited by a health plan. The preamble explained that the duty would have been shifted to the payor to request the minimum necessary information for the audit purpose, although the regulatory text did not include such a requirement. Outside of the audit context, the preamble stated that a health plan would be required, when requesting a disclosure, to limit its requests to the information required to achieve the purpose of the request; the regulation text did not include this requirement.

The preamble stated that disclosure of an entire medical record, in response to a request for something other than the entire medical record, would presumptively violate the minimum necessary standard.

This final rule significantly modifies the proposed requirements for implementing the minimum necessary standard. For all uses and many disclosures and requests for disclosures from other covered entities, we require covered entities to implement policies and procedures for ''minimum necessary'' uses and disclosures. Implementation of such policies and procedures is required in lieu of making the ''minimum necessary'' determination for each separate use or disclosure as discussed in the proposal. Disclosures to or requests by a health care provider for treatment purposes are not subject to the standard (see § 164.502).

Specifically (and as further described below), the proposed requirement for individual review of all uses of protected health information is replaced with a requirement for covered entities to implement policies and procedures that restrict access and uses based on the specific roles of members of the covered entity's workforce. Routine disclosures also are not subject to individual review; instead, covered entities must implement policies and procedures to limit the protected health information in routine disclosures to the minimum necessary to achieve the purpose of that type of disclosure. The proposed exclusion of disclosures to health plans for audit purposes is deleted and replaced with a general requirement that covered entities must limit requests to other covered entities for individually identifiable health information to what is reasonably necessary for the use or disclosure intended. The other exclusions from the standard are unchanged from the proposed rule (*e.g.,* for individuals' access to information about themselves, pursuant to an authorization initiated by the individual, for enforcement of this rule, as required by law).

The language of the basic ''standard'' itself is largely unchanged; covered entities must make reasonable efforts to use or disclose or to request from another covered entity, only the minimum amount of protected health information required to achieve the purpose of a particular use or disclosure. We delete the word ''all'' from the ''reasonable efforts'' that covered entities must take in making a ''minimum necessary'' determination. The implementation specifications are significantly modified, and differ based on whether the activity is a use or disclosure.

Similarly, a ''minimum necessary'' disclosure for oversight purposes in accordance with § 164.512(d) could include large numbers of records to allow oversight agencies to perform statistical analyses to identify deviations in payment or billing patterns, and other data analyses.

Uses of Protected Health Information

A covered entity must implement policies and procedures to identify the persons or classes of persons in the entity's workforce who need access to protected health information to carry out their duties, the category or categories of protected health information to which such persons or classes need access, and the conditions, as appropriate, that would apply to such access. Covered entities must also implement policies and procedures to limit access to only the identified persons, and only to the identified protected health information. The policies and procedures must be based on reasonable determinations regarding the persons or classes of persons who require protected health information, and the nature of the health information they require, consistent with their job responsibilities.

For example, a hospital could implement a policy that permitted nurses access to all protected health information of patients in their ward while they are on duty. A health plan could permit its underwriting analysts unrestricted access to aggregate claims information for rate setting purposes, but require documented approval from its department manager to obtain specific identifiable claims records of a member for the purpose of determining the cause of unexpected claims that could influence renewal premium rate setting.

The ''minimum necessary'' standard is intended to reflect and be consistent with, not override, professional judgment and standards. For example, we expect that covered entities will implement policies that allow persons involved in treatment to have access to the entire record, as needed.

Disclosures of Protected Health Information

For any type of disclosure that is made on a routine, recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that permit only the disclosure of the minimum protected health information reasonably necessary to achieve the purpose of the disclosure. Individual review of each disclosure is not required. Instead, under § 164.514(d)(3), these policies and procedures must identify the types of protected health information to be disclosed, the types of persons who would receive the protected health information, and the conditions that would apply for such access. We recognize that specific disclosures within a type may vary, and require that the policies address what is the norm for the type of disclosure involved. For example, a covered entity may decide to participate in research studies and therefore establish a protocol to minimize the information released for such purposes, *e.g.,* by requiring researchers requesting disclosure of data contained in paper-based records to review the paper records on-site and to

abstract only the information relevant to the research. Covered entities must develop policies and procedures (which may be standard protocols) to apply to disclosures to routinely hired types of business associates. For instance, a standard protocol could describe the subset of information that may be disclosed to medical transcription services.

For non-routine disclosures, a covered entity must develop reasonable criteria for determining, and limiting disclosure to, only the minimum amount of protected health information necessary to accomplish the purpose of the disclosure. They also must establish and implement procedures for reviewing such requests for disclosures on an individual basis in accordance with these criteria.

Disclosures to health care providers for treatment purposes are not subject to these requirements.

Covered entities' policies and procedures must provide that disclosure of an entire medical record will not be made except pursuant to policies which specifically justify why the entire medical record is needed. For instance, disclosure of all protected health information to an accreditation group would not necessarily violate the regulation, because the entire record may be the ''minimum necessary'' for its purpose; covered entities may establish policies allowing for and justifying such a disclosure. Disclosure of the entire medical record absent such documented justification is a presumptive violation of this rule.

Requests for Protected Health Information

For requests for protected health information from other covered entities made on a routine, recurring basis, the requesting covered entities' policies and procedures may establish standard protocols describing what information is reasonably necessary for the purposes and limiting their requests to only that information, in lieu of making this determination individually for each request. For all other requests, the policies and procedures must provide for review of the requests on an individualized basis. A request by a covered entity may be made in order to obtain information that will subsequently be disclosed to a third party, for example, to obtain information that will then be disclosed to a business associate for quality assessment purposes; such requests are subject to this requirement.

Covered entities' policies and procedures must provide that requests for an entire medical record will not be made except pursuant to policies which specifically justify why the entire medical record is needed. For instance, a health plan's request for all protected health information from an applicant for insurance would not necessarily violate the regulation, because the entire record may be the ''minimum necessary'' for its purpose. Covered entities may establish policies allowing for and justifying such a request. A request for the entire medical record absent such documented justification is a presumptive violation of this rule.

Reasonable Reliance

A covered entity may reasonably rely on the assertion of a requesting covered entity that it is requesting the minimum protected health information necessary for the stated purpose. A covered entity may also rely on the assertions of a professional (such as attorneys and accountants) who is a member of its workforce or its business associate regarding what protected health information he or she needs in order to provide professional services to the covered entity when such person represents that the information requested is the minimum necessary. As we proposed in the NPRM, covered entities making disclosures to public officials that are permitted under § 164.512 may rely on the representation of a public official that the information requested is the minimum necessary.

Uses and Disclosures for Research

In making a minimum necessary determination regarding the use or disclosure of protected health information for research purposes, a covered entity may reasonably rely on documentation from an IRB or privacy board describing the protected health information needed for research and consistent with the requirements of § 164.512(i), ''Uses and Disclosures for Research Purposes.'' A covered entity may also reasonably rely on a representation made by the requestor that the information is necessary to prepare a research protocol or for research on decedents. The covered entity must ensure that the representation or documentation of IRB or privacy board approval it obtains from a researcher describes with sufficient specificity the protected health information necessary for the research. Covered entities must use or disclose such protected health information in a manner that minimizes the scope of the use or disclosure.

Standards for Electronic Transactions

We clarify that under § 164.502(b)(2)(v), covered entities are not required to apply the minimum necessary standard to the required or situational data elements specified in the implementation guides for HIPAA administrative simplification standard transactions in the Transactions Rule. The standard does apply for uses or disclosures in standard transactions that are made at the option of the covered entity.

Section 164.514(e)—Marketing

In the proposed rule, we would have required covered entities to obtain the individual's authorization in order to use or disclose protected health information to market health and non-health items and services.

We have made a number of changes in the final rule that relate to marketing. In the final rule, we retain the general rule that covered entities must obtain the individual's authorization before making uses or disclosures of protected health information for marketing. However, we add a new definition of ''marketing'' that clarifies that certain activities, such as communications made by a covered entity for the purpose of describing the products and services it provides, are not marketing. See § 164.501 and the associated preamble regarding the definition of marketing. In the final rule we also permit covered entities to use and disclose protected health information for certain marketing activities without individual authorization, subject to conditions enumerated at § 164.514(e).

First, § 164.514(e) permits a covered entity to use or disclose protected health information without individual authorization to make a marketing communication if the communication occurs in a face-to-face encounter with the individual. This provision would permit a covered entity to discuss any services and products, including those of a third-party, without restriction during a face-to-face communication. A covered entity also could give the individual sample products or other information in this setting.

Second, we permit a covered entity to use or disclose protected health information without individual authorization to make marketing communications involving products or services of only nominal value. This provision ensures that covered entities do not violate the rule when they distribute calendars, pens and other merchandise that generally promotes the covered entity.

Third, we permit a covered entity to use or disclose protected health information without individual authorization to make marketing communications about the health-

related products or services of the covered entity or of a third party if the communication: (1) Identifies the covered entity as the party making the communication; (2) to the extent that the covered entity receives direct or indirect remuneration from a third-party for making the communication, prominently states that fact; (3) except in the case of a general communication (such as a newsletter), contains instructions describing how the individual may opt-out of receiving future communications about health-related products and services; and (4) where protected health information is used to target the communication about a product or service to individuals based on their health status or health condition, explains why the individual has been targeted and how the product or service relates to the health of the individual. The final rule also requires a covered entity to make a determination, prior to using or disclosing protected health information to target a communication to individuals based on their health status or condition, that the product or service may be beneficial to the health of the type or class of individual targeted to receive the communication.

This third provision accommodates the needs of health care entities to be able to discuss their own health-related products and services, or those of third parties, as part of their everyday business and as part of promoting the health of their patients and enrollees. The provision is restricted to uses by covered entities or disclosures to their business associates pursuant to a contract that requires confidentiality, ensuring that protected health information is not distributed to third parties. To provide individuals with a better understanding of how their protected health information is being used for marketing, the provision requires that the communication identify that the covered entity is the source of the communication; a covered entity may not send out information about the product of a third party without disclosing to the individual where the communication originated. We also require covered entities to disclose any direct or indirect remuneration from third parties. This requirement permits individuals to better understand why they are receiving a communication, and to weigh the extent to which their information is being used to promote their health or to enrich the covered entity. Covered entities also are required to include in their communication (unless it is a general newsletter or similar device) how the individual may prevent further communications about health-related products and services. This provision enhances individuals' control over how their information is being used. Finally, where a covered entity targets communications to individuals on the basis of their health status or condition, we require that the entity make a determination that the product or service being communicated may be beneficial to the health of the type of individuals targeted, and that the communication to the targeted individuals explain why they have been targeted and how the product or service relates to their health. This final provision balances the advantages that accrue from health care entities informing their patients and enrollees of new or valuable health products with individuals' expectations that their protected health information will be used to promote their health.

Section 164.514(f)—Fundraising

We proposed in the NPRM to require covered entities to obtain authorization from an individual in order to use the individual's protected health information for fundraising activities.

As noted in § 164.501, in the final rule we define fundraising on behalf of a covered entity to be a health care operation. In § 164.514, we permit a covered entity to use protected health information without individual authorization for fundraising on behalf of itself, provided that it limits the information that it uses to demographic information about the individual and the dates that it has provided service to the individual (see the § 164.501 discussion of ''health care operations''). In addition, we require fundraising materials to explain how the individual may opt out of any further fundraising communications, and covered entities are required to honor such requests. We permit a covered entity to disclose the limited protected health information to a business associate for fundraising on its own behalf. We also permit a covered entity to disclose the information to an institutionally related foundation.

By ''institutionally related foundation,'' we mean a foundation that qualifies as a nonprofit charitable foundation under section 501(c)(3) of the Internal Revenue Code and that has in its charter statement of charitable purposes an explicit linkage to the covered entity. An institutionally related foundation may, as explicitly stated in its charter, support the covered entity as well as other covered entities or health care providers in its community. For example, a covered hospital may disclose for fundraising on its own behalf the specified protected health information to a nonprofit foundation established for the specific purpose of raising funds for the hospital or to a foundation that has as its mission the support of the members of a particular hospital chain that includes the covered hospital. The term does not include an organization with a general charitable purpose, such as to support research about or to provide treatment for certain diseases, that may give money to a covered entity, because its charitable purpose is not specific to the covered entity.

Section 164.514(g)—Underwriting

As described under the definition of ''health care operations'' (§ 164.501), protected health information may be used or disclosed for underwriting and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits. This final rule includes a requirement, not included in the NPRM, that health plans receiving such information for these purposes may not use or disclose it for any other purpose, except as may be required by law, if the insurance or benefits contract is not placed with the health plan.

Section 164.514(h)—Verification of Identity and Authority of Persons Requesting Protected Health Information

Disclosure of Protected Health Information

We reorganize the provision regarding verification of identity of individuals requesting protected health information to improve clarity, but we retain the substance of requirements proposed in the NPRM in § 164.518(c), as follows.

The covered entity must establish and use written policies and procedures (which may be standard protocols) that are reasonably designed to verify the identity and authority of the requestor where the covered entity does not know the person requesting the protected health information. The knowledge of the person may take the form of a known place of business, address, phone or fax number, as well a known human being. Where documentation, statements or representations, whether oral or written, from the person requesting the protected health information is a condition of disclosure under this rule or other law, this verification must involve obtaining such documentation statement, or representation. In such a case, additional verification is only required where this regulation (or other law)

requires additional proof of authority and identity.

The NPRM proposed that covered entities would be permitted to rely on the required documentation of IRB or privacy board approval to constitute sufficient verification that the person making the request was a researcher and that the research is authorized. The final rule retains this provision.

For most disclosures, verifying the authority for the request means taking reasonable steps to verify that the request is lawful under this regulation. Additional proof is required by other provisions of this regulation where the request is made pursuant to § 164.512 for national priority purposes. Where the person requesting the protected health information is a public official, covered entities must verify the identity of the requester by examination of reasonable evidence, such as a written statement of identity on agency letterhead, an identification badge, or similar proof of official status. Similarly, covered entities are required to verify the legal authority supporting the request by examination of reasonable evidence, such as a written request provided on agency letterhead that describes the legal authority for requesting the release. Where § 164.512 explicitly requires written evidence of legal process or other authority before a disclosure may be made, a public official's proof of identity and the official's oral statement that the request is authorized by law are not sufficient to constitute the required reasonable evidence of legal authority; under these provisions, only the required written evidence will suffice.

In some circumstances, a person or entity acting on behalf of a government agency may make a request for disclosure of protected health information under these subsections. For example, public health agencies may contract with a nonprofit agency to collect and analyze certain data. In such cases, the covered entity is required to verify the requestor's identity and authority through examination of reasonable documentation that the requestor is acting on behalf of the government agency. Reasonable evidence includes a written request provided on agency letterhead that describes the legal authority for requesting the release and states that the person or entity is acting under the agency's authority, or other documentation, including a contract, a memorandum of understanding, or purchase order that confirms that the requestor is acting on behalf of the government agency.

In some circumstances, identity or authority will be verified as part of meeting the underlying requirements for disclosure. For example, a disclosure under § 164.512(j)(1)(i) to avert an imminent threat to safety is lawful only if made in the good faith belief that the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public, and to a person reasonably able to prevent or lessen the threat. If these conditions are met, no further verification is needed. In such emergencies, the covered entity is not required to demand written proof that the person requesting the protected health information is legally authorized. Reasonable reliance on verbal representations are appropriate in such situations.

Similarly, disclosures permitted under § 164.510(a) for facility directories may be made to the general public; the covered entity's policies and procedures do not need to address verifying the identity and authority for these disclosures. In § 164.510(b) we do not require verification of identity for persons assisting in an individual's care or for notification purposes. For disclosures when the individual is not present, such as when a friend is picking up a prescription, we allow the covered entity to use professional judgment and experience with common practice to make reasonable inferences.

Under § 164.524, a covered entity is required to give individuals access to protected health information about them (under most circumstances). Under the general verification requirements of § 164.514(h), the covered entity is required to take reasonable steps to verify the identity of the individual making the request. We do not mandate particular identification requirements (*e.g.,* drivers licence, photo ID), but rather leave this to the discretion of the covered entity. The covered entity must also establish and document procedures for verification of identity and authority of personal representatives, if not known to the entity. For example, a health care provider can require a copy of a power of attorney, or can ask questions to determine that an adult acting for a young child has the requisite relationship to the child.

In Subpart C of Part 160, we require disclosure to the Secretary for purposes of enforcing this regulation. When a covered entity is asked by the Secretary to disclose protected health information for compliance purposes, the covered entity must verify the same information that it is required to verify for any other law enforcement or oversight request for disclosure.

Use of Protected Health Information

The proposed rule's verification requirements applied to any person requesting protected health information, whether for a use or a disclosure. In the final regulation, the verification provisions apply only to disclosures of protected health information. The requirements in § 164.514(d), for implementation of policies and procedures for ''minimum necessary'' uses of protected health information, are sufficient to ensure that only appropriate persons within a covered entity will have access to protected health information.

Section 164.520—Notice of Privacy Practices for Protected Health Information

Section 164.520(a)—Right to Notice

We proposed to establish a right for individuals to receive adequate notice of how covered health care providers and health plans use and disclose protected health information, and of the individual's rights with respect to that information.

In the final regulation, we retain the general right for individuals to receive and the requirement for covered entities to produce a notice of privacy practices, with significant modifications to the content and distribution requirements.

We also modify the requirements with respect to certain covered entities. First, in § 164.500(b)(2), we clarify that a health care clearinghouse that creates or receives protected health information other than as a business associate of a covered entity must produce a notice. If a health care clearinghouse creates or receives protected health information only as a business associate of other covered entities, it is not required to produce a notice.

Second, in § 164.520(a)(2), we clarify the notice requirements with respect to group health plans. Individuals who receive health benefits under a group health plan other than through insurance are entitled to a notice from the group health plan; self-insured group health plans must maintain a notice that meets the requirements of this section and must provide the notice in accordance with the requirements of § 164.520(c). At a minimum, the self-insured group health plan's notice must describe the group health plan's privacy practices with respect to the protected health information it creates or receives through its self-insured arrangements. For example, if a group health plan maintains both fully-insured and self-insured arrangements, the group health plan must, at a minimum, maintain and provide a notice that describes its

privacy practices with respect to protected health information it creates or receives through the self-insured arrangements. This notice would be distributed to all participants in the self-insured arrangements (in accordance with § 164.520(c)(1)) and would also be available on request to other persons, including participants in the fully-insured arrangements.

Individuals who receive health benefits under a group health plan through an insurance contract (i.e., a fully-insured group health plan) are entitled to a notice from the issuer or HMO through which they receive their health benefits. The health insurance issuer or HMO must maintain and provide the notice in accordance with § 164.520(c)(1). In addition, some fully-insured group health plans are required to maintain and provide a notice of the group health plan's privacy practices. If a group health plan provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and the group health plan creates or receives protected health information in addition to summary information (as defined in § 164.504(a)) and information about individuals' enrollment in or disenrollment from a health insurance issuer or HMO offered by the group health plan, the group health plan must maintain a notice that meets the requirements of this section and must provide the notice upon request of any person. The group health plan is not required to meet the other distribution requirements of § 164.520(c)(1). Individuals enrolled in such group health plans have the right to notice of the health insurance issuer or HMO's privacy practices and, on request, to notice of the group health plan's privacy practices. If the group health plan, however, provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and the only protected health information the group health plan creates or receives is summary information (as defined in § 164.504(a)) and information about individuals' enrollment in or disenrollment from a health insurance issuer or HMO offered by the group health plan, the group health plan is not required to maintain or provide a notice under this section. In this case, the individuals enrolled in the group health plan would receive notice of the health insurance issuer or HMO's privacy practices, but would not be entitled to notice of the group health plan's privacy practices.

Third, in § 164.520(a)(3), we clarify that inmates do not have a right to notice under this section and a correctional institution that is a covered entity is not required to produce a notice. No person, including a current or former inmate, has the right to notice of such a covered entity's privacy practices.

Section 164.520(b)—Content of Notice

We proposed to require the notice to be written in plain language and contain each of the following elements: a description of the uses and disclosures expected to be made without individual authorization; statements that other uses and disclosures would be made only with the individual's authorization and that the individual could revoke such authorization; descriptions of the rights to request restrictions, inspect and copy protected health information, amend or correct protected health information, and receive an accounting of disclosures of protected health information; statements about the entity's legal requirements to protect privacy, provide notice, and adhere to the notice; a statement about how individuals would be informed of changes to the entity's policies and procedures; instructions on how to make complaints with the entity or Secretary; the name and telephone number of a contact person or office; and the date the notice was produced. We provided a model notice of information policies and procedures for covered health care providers.

In § 164.520(b), and immediately below in this preamble, we describe the notice content requirements for the final rule. As described in detail, below, we make substantial changes to the uses and disclosures of protected health information that must be described in the notice. Unlike the proposed rule, we do not include a model notice. We intend to develop further guidance on notice requirements prior to the compliance date of this rule. In this section of the final rule, we also refer to the covered entity's privacy ''practices,'' rather than its ''policies and procedures.'' The purpose of this change in vocabulary is to clarify that a covered entity's ''policies and procedures'' is a detailed documentation of all of the entity's privacy practices as required under this rule, not just those described in the notice. For example, we require covered entities to have policies and procedures implementing the requirements for ''minimum necessary'' uses and disclosures of protected health information, but these policies and procedures need not be reflected in the entity's notice. Similarly, we require covered entities to have policies and procedures for assuring individuals access to protected health information about them. While such policies and procedures will need to include documentation of the designated record sets subject to access, who is authorized to determine when information will be withheld from an individual, and similar details, the notice need only explain generally that individuals have the right to inspect and copy information about them, and tell individuals how to exercise that right.

A covered entity that adopts and follows the notice content and distribution requirements described below will have provided adequate notice. However, the requirements for the content of the notice are not intended to be exclusive. As with the rest of the rule, we specify minimum requirements, not best practices. Covered entities may want to include more detail. We note that all federal agencies must still comply with the Privacy Act of 1974. This means that federal agencies that are covered entities or have covered health care components must comply with the notice requirements of the Privacy Act as well as those included in this rule.

In addition, covered entities may want or be required to produce more than one notice in order to satisfy the notice content requirements under this rule. For example, a covered entity that conducts business in multiple states with different laws regarding the uses and disclosures that the covered entity is permitted to make without authorization may be required to produce a different notice for each state. A covered entity that conducts business both as part of an organized health care arrangement or affiliated covered entity and as an independent enterprise (e.g., a physician who sees patients through an on-call arrangement with a hospital and through an independent private practice) may want to adopt different privacy practices with respect to each line of business; such a covered entity would be required to produce a different notice describing the practices for each line of business. Covered entities must produce notices that accurately describe the privacy practices that are relevant to the individuals receiving the notice.

Required Elements

Plain Language

As in the proposed rule, we require the notice to be written in plain language. A covered entity can satisfy the plain language requirement if it makes a reasonable effort to: organize material to serve the needs of the reader; write short sentences in the active voice, using ''you'' and other pronouns; use common, everyday words in sentences; and divide material into short sections.

We do not require particular formatting specifications, such as easy-to-read design features (e.g., lists, tables, graphics, contrasting colors, and white space), type face, and font size. However, the purpose of the notice is to inform the recipients about their rights and how protected health information collected about them may be used or disclosed. Recipients who cannot understand the covered entity's notice will miss important information about their rights under this rule and about how the covered entity is protecting health information about them. One of the goals of this rule is to create an environment of open communication and transparency with respect to the use and disclosure of protected health information. A lack of clarity in the notice could undermine this goal and create misunderstandings. Covered entities have an incentive to make their notice statements clear and concise. We believe that the more understandable the notice is, the more confidence the public will have in the covered entity's commitment to protecting the privacy of health information.

It is important that the content of the notice be communicated to all recipients and therefore we encourage the covered entity to consider alternative means of communicating with certain populations. We note that any covered entity that is a recipient of federal financial assistance is generally obligated under Title VI of the Civil Rights Act of 1964 to provide material ordinarily distributed to the public in the primary languages of persons with limited English proficiency in the recipients' service areas. Specifically, this Title VI obligation provides that, where a significant number or proportion of the population eligible to be served or likely to be directly affected by a federally assisted program needs service or information in a language other than English in order to be effectively informed of or participate in the program, the recipient shall take reasonable steps, considering the scope of the program and the size and concentration of such population, to provide information in languages appropriate to such persons. For covered entities not subject to Title VI, the Title VI standards provide helpful guidance for effectively communicating the content of their notices to non-English speaking populations.

We also encourage covered entities to be attentive to the needs of individuals who cannot read. For example, an employee of the covered entity could read the notice to individuals upon request or the notice could be incorporated into a video presentation that is played in the waiting area.

Header

Unlike the proposed rule, covered entities must include prominent and specific language in the notice that indicates the importance of the notice. This is the only specific language we require covered entities to include in the notice. The header must read, ''THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.''

Uses and Disclosures

We proposed to require covered entities to describe in plain language the uses and disclosures of protected health information, and the covered entity's policies and procedures with respect to such uses and disclosures, that the health plan or covered provider expected to make without individual authorization. The covered provider or health plan would have had to distinguish between those uses and disclosures required by law and those permitted but not required by law.

We also proposed to require covered health care providers and health plans to state in the notice that all other uses and disclosures would be made only with the individual's authorization and that such authorization could be revoked. The notice would also have been required to state that the individual could request restrictions on certain uses and disclosures and that the covered entity would not be required to agree to such a request.

We significantly modify these requirements in the final rule. Covered entities must describe all uses and disclosures of protected health information that they are permitted or required to make under this rule without authorization, including those uses and disclosures subject to the consent requirements under § 164.506. If other applicable law prohibits or materially limits the covered entity's ability to make any uses or disclosures that would otherwise be permitted under the rule, the covered entity must describe only the uses and disclosures permitted under the more stringent law.

Covered entities must separately describe each purpose for which they are permitted to use or disclose protected health information under this rule without authorization, and must do so in sufficient detail to place the individual on notice of those uses and disclosures. With respect to uses and disclosures to carry out treatment, payment, and health care operations, the description must include at least one example of the types of uses and disclosures that the covered entity is permitted to make. This requirement is intended to inform individuals of all the uses and disclosures that the covered entity is legally required or permitted to make under applicable law, even if the covered entity does not anticipate actually making such uses and disclosures. We do not require covered entities to distinguish in their notices between those uses and disclosures required by law and those permitted but not required by law.

Unlike the proposed rule, we additionally require covered entities that wish to contact individuals for any of the following activities to list these activities in the notice: providing appointment reminders, describing or recommending treatment alternatives, providing information about health-related benefits and services that may be of interest to the individual, or soliciting funds to benefit the covered entity. If the covered entity does not include these statements in its notice, it is prohibited from using or disclosing protected health information for these activities without authorization. See § 164.502(i).

In addition, if a group health plan, or a health insurance issuer or HMO with respect to a group health plan, wants the option to disclose protected health information to a group health plan sponsor without authorization as permitted under § 164.504(f), the group health plan, health insurance issuer or HMO must describe that practice in its notice.

As in the proposed rule, the notice must state that all other uses and disclosures will be made only with the individual's authorization and that the individual has the right to revoke such authorization.

We anticipate this requirement will lead to significant standardization of the notice. This language could be the same for every covered entity of a particular type within a state, territory, or other locale. We encourage states, state professional associations, and other organizations to develop model language to assist covered entities in preparing their notices.

Individual Rights

As in the proposed rule, covered entities must describe individuals' rights under the rule and how individuals may exercise those rights with respect to the covered entity. Covered entities must describe each of the following rights, as provided under the rule: the right to request restrictions

on certain uses and disclosures, including a statement that the covered entity is not required to agree to a requested restriction (§ 164.522(a)); the right to receive confidential communications of protected health information (§ 164.522(b)); the right to inspect and copy protected health information (§ 164.524); the right to amend protected health information (§ 164.526); and the right to an accounting of disclosures of protected health information (§ 164.528). We additionally require the notice to describe the right of an individual, including an individual that has agreed to receive the notice electronically, to obtain a paper copy of the notice upon request.

Covered Entity's Duties

As in the proposed rule, covered entities must state in the notice that they are required by law to maintain the privacy of protected health information, to provide a notice of their legal duties and privacy practices, and to abide by the terms of the notice currently in effect. In the final rule, we additionally require the covered entity, if it wishes to reserve the right to change its privacy practices and apply the revised practices to protected health information previously created or received, to make a statement to that effect and describe how it will provide individuals with a revised notice. (See below for a more detailed discussion of a covered entity's responsibilities when it changes its privacy practices.)

Complaints

As in the proposed rule, a covered entity's notice must inform individuals about how they can lodge complaints with the covered entity if they believe their privacy rights have been violated. See § 164.530(d) and the corresponding preamble discussion for the requirements on covered entities for receiving complaints. The notice must also state that individuals may file complaints with the Secretary. In the final rule, we additionally require the notice to include a statement that the individual will not suffer retaliation for filing a complaint.

Contact

As in the proposed rule, the notice must identify a point of contact where the individual can obtain additional information about any of the matters identified in the notice.

Effective Date

The notice must include the date the notice went into effect, rather than the proposed requirement to include the date the notice was produced. The effective date cannot be earlier than the date on which the notice was first printed or otherwise published. Covered entities may wish to highlight or otherwise emphasize any material modifications that it has made, in order to help the individual recognize such changes.

Optional Elements

As described above, we proposed to require covered entities to describe the uses and disclosures of protected health information that the covered entity in fact expected to make without the individual's authorization. We did not specify any optional elements.

While the final rule requires covered entities to describe all of the types of uses and disclosures permitted or required by law (not just those that the covered entity intends to make), we also permit and encourage covered entities to include optional elements that describe the actual, more limited, uses and disclosures they intend to make without authorization. We anticipate that some covered entities will want to distinguish themselves on the basis of their more stringent privacy practices. For example, covered health care providers who routinely treat patients with particularly sensitive conditions may wish to assure their patients that, even though the law permits them to disclose information for a wide array of purposes, the covered health care provider will only disclose information in very specific circumstances, as required by law, and to avert a serious and imminent threat to health or safety. A covered entity may not include statements in the notice that purport to limit the entity's ability to make uses or disclosures that are required by law or necessary to avert a serious and imminent threat to health or safety.

As described above, if the covered entity wishes to reserve the right to change its privacy practices with respect to the more limited uses and disclosures and apply the revised practices to protected health information previously created or received, it must make a statement to that effect and describe how it will provide individuals with a revised notice. (See below for a more detailed discussion of a covered entity's responsibilities when it changes its privacy practices.)

Revisions to the Notice

We proposed to require a covered entity to adhere to the terms of its notice, and would have permitted it to change its information policies and procedures at any time. We would have required covered health care providers and health plans to update the notice to reflect material changes to the information policies and procedures described in the notice. Changes to the notice would have applied to all protected health information held by the covered entity, including information collected under prior notices. That is, we would not have require covered entities to segregate their records according to the notice in effect at the time the record was created. We proposed to prohibit covered entities from implementing a change to an information policy or procedure described in the notice until the notice was updated to reflect the change, unless a compelling reason existed to make a use or disclosure or take other action that the notice would not have permitted. In these situations, we proposed to require covered entities to document the compelling reason and, within 30 days of the use, disclosure, or other action, change its notice to permit the action.

As in the proposed rule, covered entities are required to adhere to the terms of the notice currently in effect. See § 164.502(i). When a covered entity materially changes any of the uses or disclosures, the individual's rights, the covered entity's legal duties, or other privacy practices described in its notice, it must promptly revise its notice accordingly. See § 164.520(b)(3). (Pursuant to § 164.530(i), it must also revise its policies and procedures.) Except when required by law, a material change to any term in the notice may not be implemented prior to the effective date of the notice in which such material change is reflected. In the final rule, however, we revise the circumstances under and extent to which the covered entity may revise the practices stated in the notice and apply the new practices to protected health information it created or received under prior notice.

Under § 164.530(i), a covered entity that wishes to change its practices over time without segregating its records according to the notice in effect at the time the records were created must reserve the right to do so in its notice. For example, a covered hospital that states in its notice that it will only make public health disclosures required by law, and that does not reserve the right to change this practice, is prohibited from making any discretionary public health disclosures of protected health information created or received during the effective period of that notice. If the covered hospital wishes at some point in the future to make discretionary disclosures for public health purposes, it must revise its notice to so state, and

must segregate its records so that protected health information created or received under the prior notice is not disclosed for discretionary public health purposes. This hospital may then make discretionary public health disclosures of protected health information created or received after the effective date of the revised notice.

If a second covered hospital states in its notice that it will only make public health disclosures required by law, but does reserve the right to change its practices, it is prohibited from making any discretionary public health disclosures of protected health information created or received during the effective period of that notice. If this hospital wishes at some point in the future to make discretionary disclosures for public health purposes, it must revise its notice to so state, but need not segregate its records. As of the effective date of the revised notice, it may disclose any protected health information, including information created or received under the prior notice, for discretionary public health purposes.

Section 164.530(i) and the corresponding discussion in this preamble describes requirements for revision of a covered entity's privacy policies and procedures, including the privacy practices reflected in its notice.

Section 164.520(c)—Provision of Notice

As in the proposed rule, all covered entities that are required to produce a notice must provide the notice upon request of any person. The requestor does not have to be a current patient or enrollee. We intend the notice to be a public document that people can use in choosing between covered entities.

For health plans, we proposed to require health plans to distribute the notice to individuals covered by the health plan as of the compliance date; after the compliance date, at enrollment in the health plan; after enrollment, within 60 days of a material revision to the content of the notice; and no less frequently than once every three years.

As in the proposed rule, under the final rule health plans must provide the notice to all health plan enrollees as of the compliance date. After the compliance date, health plans must provide the notice to all new enrollees at the time of enrollment and to all enrollees within 60 days of a material revision to the notice. Of course, the term ''enrollees'' includes participants and beneficiaries in group health plans.

Unlike the proposed rule, we do not require health plans to distribute the notice every three years. Instead, health plans must notify enrollees no less than once every three years about the availability of the notice and how to obtain a copy.

We also clarify that, in each of these circumstances, if a named insured and one or more dependents are covered by the same policy, the health plan can satisfy the distribution requirement with respect to the dependents by sending a single copy of the notice to the named insured. For example, if an employee of a firm and her three dependents are all covered under a single health plan policy, that health plan can satisfy the initial distribution requirement by sending a single copy of the notice to the employee rather than sending four copies, each addressed to a different member of the family.

We further clarify that if a health plan has more than one notice, it satisfies its distribution requirement by providing the notice that is relevant to the individual or other person requesting the notice. For example, a health insurance issuer may have contracts with two different group health plans. One contract specifies that the issuer may use and disclose protected health information about the participants in the group health plan for research purposes without authorization (subject to the requirements of this rule) and one contract specifies that the issuer must always obtain authorizations for these uses and disclosures. The issuer accordingly develops two notices reflecting these different practices and satisfies its distribution requirements by providing the relevant notice to the relevant group health plan participants.

We proposed to require covered health care providers with face-to-face contact with individuals to provide the notice to all such individuals at the first service delivery to the individual during the one year period after the compliance date. After this one year period, covered providers with face-to-face contact with individuals would have been required to distribute the notice to all new patients at the first service delivery. Covered providers without face-to-face contact with individuals would have been required to provide the notice in a reasonable period of time following first service delivery.

We proposed to require all covered providers to post the notice in a clear and prominent location where it would be reasonable to expect individuals seeking services from the covered provider to be able to read the notice. We would have required revisions to be posted promptly.

In the final rule, we vary the distribution requirements according to whether the covered health care provider has a direct treatment relationship with an individual, rather than whether the covered health care provider has face-to-face contact with an individual. See § 164.501 and the corresponding discussion in this preamble regarding the definition of indirect treatment relationship.

Covered health care providers that have direct treatment relationships with individuals must provide the notice to such individuals as of the first service delivery after the compliance date. This requirement applies whether the first service is delivered electronically or in person. Covered providers may satisfy this requirement by sending the notice to all of their patients at once, by giving the notice to each patient as he or she comes into the provider's office or facility or contacts the provider electronically, or by some combination of these approaches. Covered providers that maintain a physical service delivery site must prominently post the notice where it is reasonable to expect individuals seeking service from the provider to be able to read the notice. The notice must also be available on site for individuals to take on request. In the event of a revision to the notice, the covered provider must promptly post the revision and make it available on site.

Covered health care providers that have indirect treatment relationships with individuals are only required to produce the notice upon request, as described above.

The proposed rule was silent regarding electronic distribution of the notice. Under the final rule, a covered entity that maintains a web site describing the services and benefits it offers must make its privacy notice prominently available through the site.

A covered entity may satisfy the applicable distribution requirements described above by providing the notice to the individual electronically, if the individual agrees to receiving materials from the covered entity electronically and the individual has not withdrawn his or her agreement. If the covered entity knows that the electronic transmission has failed, the covered entity must provide a paper copy of the notice to the individual.

If an individual's first service delivery from a covered provider occurs electronically, the covered provider must provide electronic notice automatically and contemporaneously in response to the individual's first request for service. For example, the first time an individual requests to fill a prescription through a covered internet pharmacy, the pharmacy must automatically and contemporaneously provide the individual with the

pharmacy's notice of privacy practices. An individual that receives a covered entity's notice electronically retains the right to request a paper copy of the notice as described above. This right must be described in the notice.

We note that the Electronic Signatures in Global and National Commerce Act (Pub. L. 106–229) may apply to documents required under this rule to be provided in writing. We do not intend to affect the application of that law to documents required under this rule.

Section 164.520(d)—Joint Notice by Separate Covered Entities

The proposed rule was silent regarding the ability of legally separate covered entities to produce a single notice.

In the final rule, we allow covered entities that participate in an organized health care arrangement to comply with this section by producing a single notice that describes their combined privacy practices. See § 164.501 and the corresponding preamble discussion regarding the definition of organized health care arrangement. (We note that, under § 164.504(d), covered entities that are under common ownership or control may designate themselves as a single affiliated covered entity. Joint notice requirements do not apply to such entities. Single affiliated covered entities must produce a single notice, consistent with the requirements described above for any other covered entity. Covered entities under common ownership or control that elect not to designate themselves as a single affiliated covered entity, however, may elect to produce a joint notice if they meet the definition of an organized health care arrangement.)

The joint notice must meet all of the requirements described above. The covered entities must agree to abide by the terms of the notice with respect to protected health information created or received by the covered entities as part of their participation in the organized health care arrangement. In addition, the joint notice must reasonably identify the covered entities, or class of covered entities, to which the joint notice applies and the service delivery sites, or classes of service delivery sites, to which the joint notice applies. If the covered entities participating in the organized health care arrangement will share protected health information with each other as necessary to carry out treatment, payment, or health care operations relating to the arrangement, that fact must be stated in the notice.

Typical examples where this policy may be useful are health care facilities where physicians and other providers who have offices elsewhere also provide services at the facility (e.g. hospital staff privileges, physicians visiting their patients at a residential facility). In these cases, a single notice may cover both the physician and the facility, if the above conditions are met. The physician is required to have a separate notice covering the privacy practices at the physician's office if those practices are different than the practices described in the joint notice.

If any one of the covered entities included in the joint notice distributes the notice to an individual, as required above, the distribution requirement is met for all of the covered entities included in the joint notice.

Section 164.520(e)—Documentation

As in the proposed rule, we establish documentation requirements for covered entities subject to this provision. In the final rule, we specify that covered entities must retain copies of the notice(s) they issue in accordance with § 164.530(j). See § 164.530(j) and the corresponding preamble discussion for further description of the documentation requirements.

Section 164.522—Rights To Request Privacy Protection for Protected Health Information

Section 164.522(a)—Right of An Individual To Request Restriction of Uses and Disclosures

We proposed that individuals have the right to request that a covered health care provider restrict the use or disclosure of protected health information for treatment, payment, or health care operations. Providers would not have been required to agree to requested restrictions. However, a covered provider that agreed to a restriction could not use or disclose protected health information inconsistent with the restriction. The requirement would not have applied to permissible uses or disclosures under proposed § 164.510, including uses and disclosures in emergency circumstances under proposed § 164.510(k); when the health care services provided were emergency services; or to required disclosures to the Secretary under proposed § 164.522. We would have required covered providers to have procedures for individuals to request restrictions, for agreed-upon restrictions to be documented, for the provider to honor such restrictions, and for notification of the existence of a restriction to others to whom such protected health information is disclosed.

In the final rule, we retain the general right of an individual to request that uses and disclosures of protected health information be restricted and the requirement for covered entities to adhere to restrictions to which they have agreed. However, we include some significant changes and clarifications.

Under the final rule, we extend the right to request restrictions to health plans and to health care clearinghouses that create or receive protected health information other than as a business associate of another covered entity. All covered entities must permit individuals to request that uses and disclosures of protected health information to carry out treatment, payment, and health care operations be restricted and must adhere to restrictions to which they have agreed. A covered entity is not required to agree to a restriction. We note that restrictions between an individual and a covered entity for these or other purposes may be otherwise enforceable under other law.

Under § 164.522(a)(1)(i)(B), the right to request restrictions applies to disclosures to persons assisting in the individual's care under § 164.510(b). An individual may request that a covered entity agree not to disclose protected health information to persons assisting with the individual's care, even if such disclosure is permissible in accordance with § 164.510(b). For example, if an individual requests that a covered entity never disclose protected health information to a particular family member, and the covered entity agrees to that restriction, the covered entity is prohibited from disclosing protected health information to that family member, even if the disclosure would otherwise be permissible under § 164.510(b). We note that individuals additionally have the opportunity to agree or object to disclosures to persons assisting in the individual's care under § 164.510(b)(2). The individual retains the right to agree or object to such disclosures under § 164.510(b)(2), in accordance with the standards of that provision, regardless of whether the individual has requested a restriction under § 164.522(a). See § 164.510(b) and the corresponding preamble discussion regarding the individual's right to agree or object to disclosures to persons assisting in the individual's care.

In §§ 164.522(a)(1)(iii) and (iv) we clarify the requirements with respect to emergency treatment situations. In emergency treatment situations, a covered entity that has agreed to a restriction may use, or disclose to a health care provider, restricted protected health information that is

necessary to provide the emergency treatment. If the covered entity discloses restricted protected health information to a health care provider for emergency treatment purposes, it must request that the provider not further use or disclose the information. We expect covered entities to consider the need for access to protected health information for treatment purposes when considering a request for a restriction, to discuss this need with the individual making the request for restriction, and to agree to restrictions that will not foreseeably impede the individual's treatment. Therefore, we expect covered entities will rarely need to use or disclose restricted protected health information in emergency treatment situations. We do not intend, however, to adversely impact the delivery of health care. We therefore provide a means for the use and disclosure of restricted protected health information in emergency treatment situations, where an unexpected need for the information could arise and there is insufficient time to secure the individual's permission to use or disclose the restricted information.

In § 164.522(a)(1)(v) we clarify that restrictions are not effective under this rule to prevent uses and disclosures required by § 164.502(a)(2)(ii) or permitted under § 164.510(a) (regarding facility directories) or § 164.512 (regarding uses and disclosures for which consent, individual authorization, or opportunity to agree or object is not required). Covered entities are permitted to agree to such restrictions, but if they do so, the restrictions are not enforceable under this rule. For example, a provider who makes a disclosure under § 164.512(j)(1)(i) relating to serious and imminent threats will not be in violation of this rule even if the disclosure is contrary to a restriction agreed to under this paragraph.

In § 164.522(a)(2) we clarify a covered entity's ability to terminate a restriction to which it has agreed. A covered entity may terminate a restriction with the individual's written or oral agreement. If the individual's agreement is obtained orally, the covered entity must document that agreement. A note in the medical record or similar notation is sufficient documentation. If the individual agrees to terminate the restriction, the covered entity may use and disclose protected health information as otherwise permitted under the rule. If the covered entity wants to terminate the restriction without the individual's agreement, it may only terminate the restriction with respect to protected health information it creates or receives after it informs the individual of the termination. The restriction continues to apply to protected health information created or received prior to informing the individual of the termination. That is, any protected health information that had been collected before the termination may not be used or disclosed in a way that is inconsistent with the restriction, but any information that is collected after informing the individual of the termination of the restriction may be used or disclosed as otherwise permitted under the rule.

In § 164.522(a)(3), we clarify that a covered entity must document a restriction to which it has agreed. We do not require a specific form of documentation; a note in the medical record or similar notation is sufficient. The documentation must be retained for six years from the date it was created or the date it was last in effect, whichever is later, in accordance with § 164.530(j).

We eliminate the requirement from the NPRM for covered entities to inform persons to whom they disclose protected health information of the existence of any restriction on that information. A restriction is only binding on the covered entity that agreed to the restriction. We encourage covered entities to inform others of the existence of a restriction when it is appropriate to do so. We note, however, that disclosure of the existence of a restriction often amounts to a de facto disclosure of the restricted information itself. If a restriction does not permit a covered entity to disclose protected health information to a particular person, the covered entity must carefully consider whether disclosing the existence of the restriction to that person would also violate the restriction.

Section 164.522(b)—Confidential Communications Requirements

In the NPRM, we did not directly address the issue of whether an individual could request that a covered entity restrict the manner in which it communicated with the individual. As described above, the NPRM would have provided individuals with the right to request that health care providers restrict uses and disclosures of protected health information for treatment, payment and health care operations, but would not have required providers to agree to such a restriction.

In the final rule, we require covered entities to permit individuals to request that the covered entity provide confidential communications of protected health information about the individual. The requirement applies to communications from the covered entity to the individual, and also communications from the covered entity that would otherwise be sent to the named insured of an insurance policy that covers the individual as a dependent of the named insured. Individuals may request that the covered entity send such communications by alternative means or at alternative locations. For example, an individual who does not want his or her family members to know about a certain treatment may request that the provider communicate with the individual about that treatment at the individual's place of employment, by mail to a designated address, or by phone to a designated phone number. Similarly, an individual may request that the provider send communications in a closed envelope rather than a post card, as an ''alternative means.'' Covered health care providers must accommodate all reasonable requests. Health plans must accommodate all reasonable requests, if the individual clearly states that the disclosure of all or part of the protected health information could endanger the individual. For example, if an individual requests that a health plan send explanations of benefits about particular services to the individual's work rather than home address because the individual is concerned that a member of the individual's household (e.g., the named insured) might read the explanation of benefits and become abusive towards the individual, the health plan must accommodate the request.

The reasonableness of a request made under this paragraph must be determined by a covered entity solely on the basis of the administrative difficulty of complying with the request and as otherwise provided in this section. A covered health care provider or health plan cannot refuse to accommodate a request based on its perception of the merits of the individual's reason for making the request. A covered health care provider may not require the individual to provide a reason for the request as a condition of accommodating the request. As discussed above, a health plan is not required to accommodate a request unless the individual indicates that the disclosure could endanger the individual. If the individual indicates such endangerment, however, the covered entity cannot further consider the individual's reason for making the request in determining whether it must accommodate the request.

A covered health care provider or health plan may refuse to accommodate a request, however, if the individual has

not provided information as to how payment, if applicable, will be handled, or if the individual has not specified an alternative address or method of contact.

Section 164.524—Access of Individuals to Protected Health Information

Section 164.524(a)—Right of Access

In the NPRM, we proposed to establish a right for individuals to access (*i.e.,* inspect and obtain a copy of) protected health information about them maintained by a covered provider or health plan, or its business partners, in a designated record set.

As in the proposed rule, in the final rule we provide that individuals have a right of access to protected health information that is maintained in a designated record set. This right applies to health plans, covered health care providers, and health care clearinghouses that create or receive protected health information other than as a business associate of another covered entity (see § 164.500(b)). In the final rule, however, we modify the definition of designated record set. For a discussion of the significant changes made to the definition of designated record set, see § 164.501 and the corresponding preamble.

Under the revised definition, individuals have a right of access to any protected health information that is used, in whole or in part, to make decisions about individuals. This information includes, for example, information used to make health care decisions or information used to determine whether an insurance claim will be paid. Covered entities often incorporate the same protected health information into a variety of different data systems, not all of which will be utilized to make decisions about individuals. For example, information systems that are used for quality control or peer review analyses may not be used to make decisions about individuals. In that case, the information systems would not fall within the definition of designated record set. We do not require entities to grant an individual access to protected health information maintained in these types of information systems.

Duration of the Right of Access

As in the proposed rule, covered entities must provide access to individuals for as long as the protected health information is maintained in a designated record set.

Exceptions to the Right of Access

In the NPRM, we proposed to establish a right for individuals to access any protected health information maintained in a designated record set. Though we proposed to permit covered entities to deny access in certain situations relating to the particular individual requesting access, we did not specifically exclude any protected health information from the right of access.

In the final rule, we specify three types of information to which individuals do not have a right of access, even if the information is maintained in a designated record set. They are psychotherapy notes, information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding, and certain protected health information maintained by a covered entity that is subject to or exempted from the Clinical Laboratory Improvements Amendments of 1988 (CLIA). Covered entities may, but are not required to, provide access to this information.

First, unlike the proposed rule, we specify that individuals do not have a right of access to psychotherapy notes.

Second, individuals do not have a right of access to information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding. In the NPRM, we would have permitted covered entities to deny a request for access to protected health information complied in reasonable anticipation of, or for use in, a legal proceeding. We change the language in the final rule to clarify that a legal proceeding includes civil, criminal, and administrative actions and proceedings. In the final rule, we clarify that an individual does not have a right to this information by including it in the list of exceptions rather than stating that a covered entity may deny access to this information. Under this exception, the covered entity may deny access to any information that relates specifically to legal preparations but may not deny access to the individual's underlying health information. We do not intend to require covered entities to provide access to documents protected by attorney work-product privilege nor do we intend to alter rules of discovery.

Third, unlike the proposed rule, individuals do not have a right of access to protected health information held by clinical laboratories if CLIA prohibits such access. CLIA states that clinical laboratories may provide clinical laboratory test records and reports only to ''authorized persons,'' as defined primarily by state law. The individual who is the subject of the information is not always included in this set of authorized persons. When an individual is not an authorized person, this restriction effectively prohibits the clinical laboratory from providing an individual access to this information. We do not intend to preempt CLIA and, therefore, do not require covered clinical laboratories to provide an individual access to this information if CLIA prohibits them from doing so. We note, however, that individuals have the right of access to this information if it is maintained by a covered health care provider, clearinghouse, or health plan that is not subject to CLIA.

Finally, unlike the proposed rule, individuals do not have access to protected health information held by certain research laboratories that are exempt from the CLIA regulations. The CLIA regulations specifically exempt the components or functions of ''research laboratories that test human specimens but do not report patient specific results for the diagnosis, prevention or treatment of any disease or impairment of, or the assessment of the health of individual patients.'' 42 CFR 493.3(a)(2). If subject to the access requirements, these laboratories, or the applicable components of them, would be forced to comply with the CLIA regulations once they provided an individual with the access under this privacy rule. Therefore, to alleviate this additional regulatory burden, we have exempted these laboratories, or the relevant components of them, from the access requirements of this regulation.

Grounds for Denial of Access

In the NPRM we proposed to permit covered health care providers and health plans to deny an individual access to inspect and copy protected health information about them for five reasons: (1) a licensed health care professional determined the inspection and copying was reasonably likely to endanger the life or physical safety of the individual or another person; (2) the information was about another person (other than a health care provider) and a licensed health care professional determined the inspection and copying was reasonably likely to cause substantial harm to that other person; (3) the information was obtained under a promise of confidentiality from someone other than a health care provider and the inspection and copying was likely to reveal the source of the information; (4) the information was obtained by a covered provider in the course of a clinical trial, the individual agreed to the denial of access in consenting to participate in the trial, and the trial was in progress; and (5) the information was compiled in reasonable anticipation of, or for use in, a legal

proceeding. In the NPRM, covered entities would not have been permitted to use these grounds to deny individuals access to protected health information that was also subject to the Privacy Act.

In the final rule, we retain all of these grounds for denial, with some modifications. One of the proposed grounds for denial (regarding legal proceedings) is retained as an exception to the right of access. (See discussion above.) We also include additional grounds for denial and create a right for individuals to request review of certain denials.

There are five types of denials covered entities may make without providing the individual with a right to have the denial reviewed.

First, a covered entity may deny an individual access to any information that is excepted from the right of access under § 164.524(a)(1). (See discussion above.)

Second, we add a new provision that permits a covered entity that is a correctional institution or covered health care provider acting under the direction of a correctional institution to deny an inmate's request to obtain a copy of protected health information if obtaining a copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or other inmates or the safety of any officer, employee or other person at the correctional institution or responsible for the transporting of the inmate. This ground for denial is restricted to an inmate's request to obtain a copy of protected health information. If an inmate requests inspection of protected health information, the request must be granted unless one of the other grounds for denial applies. The purpose for this exception, and the reason that the exception is limited to denying an inmate a copy and not to denying a right to inspect, is to give correctional institutions the ability to maintain order in these facilities and among inmates without denying an inmate the right to review his or her protected health information.

Third, as in the proposed rule, a covered entity may deny an individual access to protected health information obtained by a covered provider in the course of research that includes treatment of the research participants, while such research is in progress. For this exception to apply, the individual must have agreed to the denial of access in conjunction with the individual's consent to participate in the research and the covered provider must have informed the individual that the right of access will be reinstated upon completion of the research. If either of these conditions is not met, the individual has the right to inspect and copy the information (subject to the other exceptions we provide here). In all cases, the individual has the right to inspect and copy the information after the research is complete.

As with all the grounds for denial, covered entities are not required to deny access under the research exception. We expect all researchers to maintain a high level of ethical consideration for the welfare of research participants and provide access in appropriate circumstances. For example, if a participant has a severe adverse reaction, disclosure of information during the course of the research may be necessary to give the participant adequate information for proper treatment decisions.

Fourth, we clarify the ability of a covered entity to deny individuals access to protected health information that is also subject to the Privacy Act. In the final rule, we specify that a covered entity may deny an individual access to protected health information that is contained in records that are subject to the Privacy Act if such denial is permitted under the Privacy Act. This ground for denial exists in addition to the other grounds for denial available under this rule. If an individual requests access to protected health information that is also subject to the Privacy Act, a covered entity may deny access to that information for any of the reasons permitted under the Privacy Act and for any of the reasons permitted under this rule.

Fifth, as in the proposed rule, a covered entity may deny an individual access to protected health information if the covered entity obtained the requested information from someone other than a health care provider under a promise of confidentiality and such access would be reasonably likely to reveal the source of the information. This provision is intended to preserve a covered entity's ability to maintain an implicit or explicit promise of confidentiality. A covered entity may not, however, deny access to protected health information when the information has been obtained from a health care provider. An individual is entitled to have access to all information about him or her generated by the health care system (apart from the other exceptions we provide here). Confidentiality promises to health care providers should not interfere with that access.

As in the proposed rule, a covered entity may deny access to protected health information under certain circumstances in which the access may harm the individual or others. In the final rule, we specify that a covered entity may only deny access for these reasons if the covered entity provides the individual with a right to have the denial reviewed. (See below for a discussion of the right to review.)

There are three types of denials for which covered entities must provide the individual with a right to review. A denial under these provisions requires a determination by a licensed health care professional (such as a physician, physician's assistant, or nurse) based on an assessment of the particular circumstances and current professional medical standards of harm. Therefore, when the request is made to a health plan or clearinghouse, the covered entity will need to consult with a licensed health care professional before denying access under this provision.

First, as in the proposed rule, covered entities may deny individuals access to protected health information about them if a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person. The most commonly cited example is when an individual exhibits suicidal or homicidal tendencies. If a licensed health care professional determines that an individual exhibits such tendencies and that permitting inspection or copying of some of the individual's protected health information is reasonably likely to result in the individual committing suicide, murder, or other physical violence, then the health care professional may deny the individual access to that information. Under this reason for denial, covered entities may not deny access on the basis of the sensitivity of the health information or the potential for causing emotional or psychological harm.

Second, as in the proposed rule, covered entities may deny an individual access to protected health information if the information requested makes reference to someone other than the individual (and other than a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause serious harm to that other person. On some occasions when health information about one person is relevant to the care of another, a physician may incorporate it into the latter's record, such as information from group therapy sessions and information about illnesses with a genetic component. This provision permits a covered entity to withhold information in such cases if

the release of such information is reasonably likely to cause substantial physical, emotional, or psychological harm.

Third, we add a new provision regarding denial of access requested by personal representatives. Under § 164.502(g), a person that is a personal representative of an individual may exercise the rights of the individual, including the right to inspect and copy protected health information about the individual that is relevant to such person's representation. The provision permits covered entities to refuse to treat a personal representative as the individual, generally, if the covered entity has a reasonable belief that the individual has been or will be subjected to domestic violence, abuse or neglect by the personal representative, or that treating the personal representative as the individual may endanger the individual and, in its professional judgment, the covered entity decides that it is not in the best interest of the individual to treat such person as the personal representative.

In addition to that provision, we add a new provision at § 164.524(a)(3)(iii) to clarify that a covered entity may deny a request to inspect or copy protected health information if the information is requested by a personal representative of the individual and a licensed health care professional has determined that, in the exercise of professional judgment, such access is reasonably likely to cause substantial harm to the individual who is the subject of the information or to another person. The health care professional need not have a reasonable belief that the personal representative has abused or neglected the individuals and the harm that is likely to result need not be limited to the individual who is the subject of the requested protected health information. Therefore, a covered entity can recognize a person as a personal representative but deny such person access to protected health information as a personal representative.

We do not intend these provisions to create a legal duty for the covered entity to review all of the relevant protected health information before releasing it. Rather, we are preserving the flexibility and judgment of covered entities to deny access under appropriate circumstances. Denials are not mandatory; covered entities may always elect to provide requested health information to the individual. For each request by an individual, the covered entity may provide all of the information requested or evaluate the requested information, consider the circumstances surrounding the individual's request, and make a determination as to whether that request should be granted or denied, in whole or in part, in accordance with one of the reasons for denial under this rule. We intend to create narrow exceptions to the right of access and we expect covered entities to employ these exceptions rarely, if at all. Covered entities may only deny access for the reasons specifically provided in the rule.

Review of a Denial of Access

In the NPRM, we proposed to require covered entities, when denying an individual's request for access, to inform the individual of how to make a complaint to the covered entity and the Secretary.

We retain in the final rule the proposed approach (see below). In addition, if the covered entity denies the request on the basis of one of the reviewable grounds for denial described above, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny access. The covered entity must provide access in accordance with the reviewing official's determination. (See below for further description of the covered entity's requirements under § 164.524(d)(4) if the individual requests a review of denial of access.)

Section 164.524(b)—Requests for Access and Timely Action

In the NPRM, we proposed to require covered health care providers and health plans to provide a means for individuals to request access to protected health information about them. We proposed to require covered health care providers and health plans to take action on a request for access as soon as possible, but not later than 30 days following the request.

As in the proposed rule, the final rule requires covered entities to permit an individual to request access to inspect or to obtain a copy of the protected health information about the individual that is maintained in a designated record set. We additionally permit covered entities to require individuals to make requests for access in writing, if the individual is informed of this requirement.

In the final rule, we eliminate the requirement for the covered entity to act on a request as soon as possible. We recognize that circumstances may arise in which an individual will request access on an expedited basis. We encourage covered entities to have procedures in place for handling such requests. The time limitation is intended to be an outside deadline, rather than an expectation.

In the final rule, covered entities must act on a request for access within 30 days of receiving the request if the information is maintained or accessible on-site. Covered entities must act on a request for access within 60 days of receiving the request if the information is not maintained or accessible on-site. If the covered entity is unable to act on a request within the applicable deadline, it may extend the deadline by no more than 30 days by providing the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request. This written statement describing the extension must be provided within the standard deadline. A covered entity may only extend the deadline once per request for access. This provision permits a covered entity to take a total of up to 60 days to act on a request for access to information maintained on-site and up to 90 days to act on a request for access to information maintained off-site.

The requirements for a covered entity to comply with or deny a request for access, in whole or in part, are described below.

Section 164.524(c)—Provision of Access

In the NPRM, we proposed to require covered health care providers and health plans, upon accepting a request for access, to notify the individual of the decision and of any steps necessary to fulfill the request; to provide the information requested in the form or format requested, if readily producible in such form or format; and to facilitate the process of inspection and copying.

We generally retain the proposed approach in the final rule. If a covered entity accepts a request, in whole or in part, it must notify the individual of the decision and provide the access requested. Individuals have the right both to inspect and to copy protected health information in a designated record set. The individual may choose whether to inspect the information, to copy the information, or to do both.

In the final rule, we clarify that if the same protected health information is maintained in more than one designated record set or at more than one location, the covered entity is required to produce the information only once per request for access. We intend this provision to reduce covered entities' burden in complying with requests without reducing individuals' access to protected health information. We note that summary information and reports

are not the same as the underlying information on which the summary or report was based. Individuals have the right to obtain access both to summaries and to the underlying information. An individual retains the right of access to the underlying information even if the individual requests access to, or production of, a summary. (See below regarding requests for summaries.)

The covered entity must provide the information requested in the form or format requested if it is readily producible in such form or format. For example, if the covered entity maintains health information electronically and the individual requests an electronic copy, the covered entity must accommodate such request, if possible. Additionally, we specify that if the information is not available in the form or format requested, the covered entity must produce a readily readable hard copy of the information or another form or format to which the individual and covered entity can agree. If the individual agrees, including agreeing to any associated fees (see below), the covered entity may provide access to a summary of information rather than all protected health information in designated record sets. Similarly, a covered entity may provide an explanation in addition to the protected health information, if the individual agrees in advance to the explanation and any associated fees.

The covered entity must provide the access requested in a timely manner, as described above, and arrange for a mutually convenient time and place for the individual to inspect the protected health information or obtain a copy. If the individual requests that the covered entity mail a copy of the information, the covered entity must do so, and may charge certain fees for copying and mailing. For requests to inspect information that is maintained electronically, the covered entity may print a copy of the information and allow the individual to view the print-out on-site. Covered entities may discuss the request with the individual as necessary to facilitate the timely provision of access. For example, if the individual requested a copy of the information by mail, but the covered entity is able to provide the information faster by providing it electronically, the covered entity may discuss this option with the individual.

We proposed in the NPRM to permit the covered entity to charge a reasonable, cost-based fee for copying the information.

We clarify this provision in the final rule. If the individual requests a copy of protected health information, a covered entity may charge a reasonable, cost-based fee for the copying, including the labor and supply costs of copying. If hard copies are made, this would include the cost of paper. If electronic copies are made to a computer disk, this would include the cost of the computer disk. Covered entities may not charge any fees for retrieving or handling the information or for processing the request. If the individual requests the information to be mailed, the fee may include the cost of postage. Fees for copying and postage provided under state law, but not for other costs excluded under this rule, are presumed reasonable. If such per page costs include the cost of retrieving or handling the information, such costs are not acceptable under this rule.

If the individual requests an explanation or summary of the information provided, and agrees in advance to any associated fees, the covered entity may charge for preparing the explanation or summary as well.

The inclusion of a fee for copying is not intended to impede the ability of individuals to copy their records. Rather, it is intended to reduce the burden on covered entities. If the cost is excessively high, some individuals will not be able to obtain a copy. We encourage covered entities to limit the fee for copying so that it is within reach of all individuals.

We do not intend to affect the fees that covered entities charge for providing protected health information to anyone other than the individual. For example, we do not intend to affect current practices with respect to the fees one health care provider charges for forwarding records to another health care provider for treatment purposes.

Section 164.524(d)—Denial of Access

We proposed in the NPRM to require a covered health care provider or health plan that elects to deny a request for inspection or copying to make any other protected health information requested available to the individual to the extent possible, consistent with the denial.

In the final rule, we clarify the proposed approach. A covered entity that denies access, in whole or in part, must, to the extent possible, give the individual access to any other protected health information requested after excluding the protected health information to which the covered entity has a ground to deny access. We intend covered entities to redact or otherwise exclude only the information that falls within one or more of the denial criteria described above and to permit inspection and copying of all remaining information, to the extent it is possible to do so.

We also proposed to require covered providers and health plans, upon denying a request for access in whole or in part, to provide the individual with a written statement in plain language of the basis for the denial and how the individual could make a complaint to the covered entity or the Secretary.

We retain the proposed approach. A covered entity that denies access, in whole or in part, must provide the individual with a written denial in plain language that explains the basis for the denial. The written denial could include a direct reference to the section of the regulation relied upon for the denial, but the regulatory citation alone does not sufficiently explain the reason for the denial. The written denial must also describe how the individual can complain to the covered entity and the Secretary and must include the name or title and the telephone number of the covered entity's contact person or office that is responsible for receiving complaints.

In the final rule, we impose two additional requirements when the covered entity denies access, in whole or in part. First, if a covered entity denies a request on the basis of one of the reviewable grounds for denial, the written denial must describe the individual's right to a review of the denial and how the individual may exercise this right. Second, if the covered entity denies the request because it does not maintain the requested information, and the covered entity knows where the requested information is maintained, the covered entity must inform the individual where to direct the request for access.

Finally, we specify a covered entity's responsibilities when an individual requests a review of a denial. If the individual requests a review of a denial made under § 164.524(a)(3), the covered entity must designate a licensed health care professional to act as the reviewing official. This reviewing official must not have been involved in the original decision to deny access. The covered entity must promptly refer a request for review to the designated reviewing official. The reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards in § 164.524(a)(3). The covered entity must promptly provide the individual with written notice of the reviewing official's decision and otherwise carry out the decision in accordance with the requirements of this section.

Section 164.524(e)—Policies, Procedures, and Documentation

As in the proposed rule, we establish documentation requirements for covered entities that are subject to this provision. In accordance with § 164.530(j), the covered entity must retain documentation of the designated record sets that are subject to access by individuals and the titles of the persons or offices responsible for receiving and processing requests for access by individuals.

Section 164.526—Amendment of Protected Health Information

Section 164.526(a)—Right to Amend

In proposed § 164.516, we proposed to establish the individual's right to request a covered health care provider or health plan to amend or correct protected health information about the individual for as long as the covered entity maintains the information.

In § 164.526 of the final rule, we retain the general proposed approach, but establish an individual's right to have the covered entity amend, rather than amend or correct, protected health information. This right applies to protected health information and records in a designated record set for as long as the information is maintained in the designated record set. In the final rule, covered health care providers, health plans, and health care clearinghouses that create or receive protected health information other than as a business associate must comply with these requirements.

Denial of Amendment

We proposed to permit a covered health care provider or health plan to deny a request for amendment if it determined that the protected health information that was the subject of the request was not created by the covered provider or health plan, would not be available for inspection and copying under proposed § 164.514, or was accurate and complete. A covered entity would have been permitted, but not required, to deny a request if any of these conditions were met.

As in the proposed rule, the final rule permits a covered entity to deny a request for amendment if the covered entity did not create the protected health information or record that is the subject of the request for amendment. We add one exception to this provision: if the individual provides a reasonable basis to believe that the originator of the protected health information is no longer available to act on the requested amendment, the covered entity must address the request for amendment as though the covered entity had created the information.

As in the proposed rule, a covered entity also may deny a request for amendment if the protected health information that is the subject of the request for amendment is not part of a designated record set or would not otherwise be available for inspection under § 164.524. We eliminate the ability to deny a request for amendment if the information or record that is the subject of the request would not be available for copying under the rule. Under § 164.524(a)(2)(ii), an inmate may be denied a copy of protected health information about the inmate. We intend to preserve an inmate's ability to request amendments to information, even if a copy of the information would not be available to the inmate, subject to the other exceptions provided in this section.

Finally, as in the proposed rule, a covered entity may deny a request for amendment if the covered entity determines that the information in dispute is accurate and complete. We draw this concept from the Privacy Act of 1974, governing records held by federal agencies, which permits an individual to request correction or amendment of a record ''which the individual believes is not accurate, relevant, timely, or complete.'' (5 U.S.C. 552a(d)(2)). We adopt the standards of ''accuracy'' and ''completeness'' and draw on the clarification and analysis of these terms that have emerged in administrative and judicial interpretations of the Privacy Act during the last 25 years. We note that for federal agencies that are also covered entities, this rule does not diminish their present obligations under the Privacy Act of 1974.

This right is not intended to interfere with medical practice or to modify standard business record keeping practices. Perfect records are not required. Instead, a standard of reasonable accuracy and completeness should be used. In addition, this right is not intended to provide a procedure for substantive review of decisions such as coverage determinations by payors. It is intended only to affect the content of records, not the underlying truth or correctness of materials recounted therein. Attempts under the Privacy Act of 1974 to use this mechanism as a basis for collateral attack on agency determinations have generally been rejected by the courts. The same results are intended here.

Section 164.526(b)—Requests for Amendment and Timely Action

We proposed to require covered health care providers and health plans to provide a means for individuals to request amendment of protected health information about them. Under the NPRM, we would have required covered health care providers and health plans to take action on a request for amendment or correction within 60 days of the request.

As in the proposed rule, covered entities must permit individuals to request that the covered entity amend protected health information about them. We also permit certain specifications for the form and content of the request. If a covered entity informs individuals of such requirements in advance, a covered entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment. If the covered entity imposes such a requirement and informs individuals of the requirement in advance, the covered entity is not required to act on an individual's request that does not meet the requirements.

We retain the requirement for covered entities to act on a request for amendment within 60 days of receipt of the request. In the final rule, we specify the nature of the action the covered entity must take within the time frame. The covered entity must inform the individual, as described below, that the request has been either accepted or denied, in whole or in part. It must also take certain actions pursuant to its decision to accept or deny the request, as described below. If the covered entity is unable to meet the deadline, the covered entity may extend the deadline by no more than 30 days. The covered entity must inform the individual in writing, within the initial 60-day period, of the reason for the delay and the date by which the covered entity will complete its action on the request. A covered entity may only extend the deadline one time per request for amendment.

Section 164.526(c)—Accepting the Amendment

If a covered health care provider or health plan accepted a request for amendment, in whole or in part, we proposed to require the covered entity to make the appropriate change. The covered entity would have had to identify the challenged entries as amended or corrected and indicate the location of the amended or corrected information.

We also proposed to require the covered provider or health plan to make reasonable efforts to notify certain entities of the amendment: 1) entities the individual identified as needing to be notified and 2) entities the covered provider or health plan knew had received the erroneous or incomplete information and who may have relied, or could foreseeably rely, on such information to the detriment of the individual.

The covered provider or health plan would also have been required to notify the individual of the decision to amend the information.

As in the proposed rule, if a covered entity accepts an individual's request for amendment or correction, it must make the appropriate amendment. In the final rule, we clarify that, at a minimum, the covered entity must identify the records in the designated record set that are affected by the amendment and must append or otherwise provide a link to the location of the amendment. We do not require covered entities to expunge any protected health information. Covered entities may expunge information if doing so is consistent with other applicable law and the covered entity's record keeping practices.

We alter some of the required procedures for informing the individual and others of the accepted amendment. As in the proposed rule, the covered entity must inform individuals about accepted amendments. In the final rule, the covered entity must obtain the individual's agreement to have the amended information shared with certain persons. If the individual agrees, the covered entity must make reasonable efforts to provide a copy of the amendment within a reasonable time to: (1) Persons the individual identifies as having received protected health information about the individual and needing the amendment; and (2) persons, including business associates, that the covered entity knows have the unamended information and who may have relied, or could foreseeably rely, on the information to the detriment of the individual. For example, a covered entity must make reasonable efforts to inform a business associate that uses protected health information to make decisions about individuals about amendments to protected health information used for such decisions.

Section 164.526(d)—Denying the Amendment

If a covered health care provider or health plan denied a request for amendment, in whole or in part, we proposed to require the covered entity to provide the individual with a written statement in plain language of the basis for the denial, a description of how the individual could submit a written statement of disagreement with the denial, and a description of how the individual could make a complaint with the covered entity and the Secretary.

We proposed to require covered health care providers and health plans to have procedures to permit the individual to file a written statement of disagreement with the denial and to include the covered entity's statement of denial and the individual's statement of disagreement with any subsequent disclosure of the disputed information. Covered entities would have been permitted to establish a limit to the length of the individual's statement of disagreement and to summarize the statement if necessary. We also proposed to permit covered entities to provide a rebuttal to the individual's statement with future disclosures.

As in the proposed rule, if a covered entity denies a request for amendment, it must provide the individual with a statement of denial written in plain language. The written denial must include the basis for the denial, how the individual may file a written statement disagreeing with the denial, and how the individual may make a complaint to the covered entity and the Secretary.

In the final rule, we additionally require the covered entity to inform individuals of their options with respect to future disclosures of the disputed information in order to ensure that an individual is aware of his or her rights. The written denial must state that if the individual chooses not to file a statement of disagreement, the individual may request that the covered entity include the individual's request for amendment and the covered entity's denial of the request with any future disclosures of the protected health information that is the subject of the requested amendment.

As in the proposed rule, the covered entity must permit the individual to submit a written statement disagreeing with the denial and the basis of such disagreement. The covered entity may reasonably limit the length of a statement of disagreement and may prepare a written rebuttal to the individual's statement of disagreement. If the covered entity prepares a rebuttal, it must provide a copy to the individual.

The covered entity must identify the record or protected health information that is the subject of the disputed amendment and append or otherwise link the following information to the designated record set: the individual's request for amendment, the covered entity's denial of the request, the individual's statement of disagreement (if any), and the covered entity's rebuttal (if any). If the individual submits a written statement of disagreement, all of the appended or linked information, or an accurate summary of it, must be included with any subsequent disclosure of the protected health information to which the disagreement relates. If the individual does not submit a written statement of disagreement, the covered entity must include the appended or linked information only if the individual requests that the covered entity do so.

In the final rule, we clarify that when a subsequent disclosure is a standard transaction adopted under the Transactions Rule that cannot accommodate the additional materials described above, the covered entity may separately disclose the additional material to the recipient of the transaction.

Section 164.526(e)—Actions on Notices of Amendment

We proposed to require any covered entity that received a notification of amendment to have procedures in place to make the amendment in any of its designated record sets and to notify its business associates, if appropriate, of amendments.

We retain the proposed approach in the final rule. If a covered entity receives a notification of amended protected health information from another covered entity as described above, the covered entity must make the necessary amendment to protected health information in designated record sets it maintains. In addition, covered entities must require their business associates who receive such notifications to incorporate any necessary amendments to designated record sets maintained on the covered entity's behalf. (See § 164.504 regarding business associate requirements.)

Section 164.526(f)—Policies, Procedures, and Documentation

As in the proposed rule, we establish documentation requirements for covered entities subject to this provision. In accordance with § 164.530(j), the covered entity must document the titles of the persons or offices responsible for receiving and processing requests for amendment.

§ 164.528—Accounting of Disclosures of Protected Health Information

Right to an Accounting of Disclosures

We proposed in the NPRM to grant individuals a right to receive an

accounting of all disclosures of protected health information about them by a covered entity for purposes other than treatment, payment, and health care operations. We proposed this right to exist for as long as the covered entity maintained the protected health information.

We also proposed that individuals would not have a right to an accounting of disclosures to health oversight or law enforcement agencies if the agency provided a written request for exclusion for a specified time period and the request stated that access by the individual during that time period would be reasonably likely to impede the agency's activities.

We generally retain the proposed approach in the final rule. As in the proposed rule, individuals have a right to receive an accounting of disclosures made by a covered entity, including disclosures by or to a business associate of the covered entity, for purposes other than treatment, payment, and health care operations, subject to certain exceptions as discussed below.

We revise the duration of this right under the final rule. Individuals have a right to an accounting of the applicable disclosures that have been made in the 6 year period prior to the date of a request for an accounting. We additionally clarify in § 164.528(b)(1) that an individual may request, and a covered entity may then provide, an accounting of disclosures for a period of time less than 6 years from the date of the request. For example, an individual could request an accounting only of disclosures that occurred during the year prior to the request.

In the final rule, we exclude several additional types of disclosures from the accounting requirement. Covered entities are not required to include in the accounting disclosures to the individual as provided in § 164.502; disclosures for facility directories, disclosures to persons involved in the individual's care, or other disclosures for notification purposes as provided in § 164.510; disclosures for national security or intelligence purposes as provided in § 164.512(k)(2); disclosures to correctional institutions or law enforcement officials as provided in § 164.512(k)(5); or any disclosures that were made by the covered entity prior to the compliance date of the rule for that covered entity.

We retain the time-limited exclusion for disclosures to health oversight and law enforcement agencies, but require rather than permit the exclusion for the specified time period. Covered entities must exclude disclosures to a health oversight agency or law enforcement official from the accounting for the time period specified by the applicable agency or official if the agency or official provides the covered entity with a statement that inclusion of the disclosure(s) in the accounting to the individual during that time period would be reasonably likely to impede the agency or official's activities. The agency or official's statement must specifically state how long the information must be excluded. At the expiration of that period, the covered entity is required to include the disclosure(s) in an accounting for the individual. If the agency or official's statement is made orally, the covered entity must document the identity of the agency or official who made the statement and must exclude the disclosure(s) for no longer than 30 days from the date of the oral statement, unless a written statement is provided during that time. If the agency or official provides a written statement, the covered entity must exclude the disclosure(s) for the time period specified in the written statement.

Content of the Accounting

We proposed in the NPRM to require the accounting to include all disclosures as described above, including disclosures authorized by the individual. The accounting would have been required to contain the date of each disclosure; the name and address of the organization or person who received the protected health information; a brief description of the information disclosed; and copies of all requests for disclosures. For disclosures other than those made at the request of the individual, the accounting would have also included the purpose for which the information was disclosed.

We generally retain the proposed approach in the final rule, but do not require covered entities to make copies of authorizations or other requests for disclosures available with the accounting. Instead, we require the accounting to contain a brief statement of the purpose of the disclosure. The statement must reasonably inform the individual of the basis for the disclosure. In lieu of the statement of purpose, a covered entity may include a copy of the individual's authorization under § 164.508 or a copy of a written request for disclosure, if any, under § 164.502(a)(2)(ii) or § 164.512. We also clarify that covered entities are only required to include the address of the recipient of the disclosed protected health information if the covered entity knows the address.

We add a provision allowing for a summary accounting of recurrent disclosures. For multiple disclosures to the same recipient pursuant to a single authorization under § 164.508 or for a single purpose under §§ 164.502(a)(2)(ii) or 164.512, the covered entity may provide a summary accounting addressing the series of disclosures rather than a detailed accounting of each disclosure in the series. In this circumstance, a covered entity may limit the accounting of the series of disclosures to the following information: the information otherwise required above for the first disclosure in the series during the accounting period; the frequency, periodicity, or number of disclosures made during the accounting period; and the date of the most recent disclosure in the series. For example, if under § 164.512(b), a covered entity discloses the same protected health information to a public health authority for the same purpose every month, it can account for those disclosures by including in the accounting the date of the first disclosure, the public health authority to whom the disclosures were made and the public health authority's address, a brief description of the information disclosed, a brief description of the purpose of the disclosures, the fact that the disclosures were made every month during the accounting period, and the date of the most recent disclosure.

Provision of the Accounting

We proposed in the NPRM to require covered entities to provide individuals with an accounting of disclosures as soon as possible, but not later than 30 days following receipt of the request for the accounting.

In the final rule, we eliminate the requirement for the covered entity to act as soon as possible. We recognize that circumstances may arise in which an individual will request an accounting on an expedited basis. We encourage covered entities to implement procedures for handling such requests. The time limitation is intended to be an outside deadline, rather than an expectation. We expect covered entities always to be attentive to the circumstances surrounding each request and to respond in an appropriate time frame.

In the final rule, covered entities must provide a requested accounting no later than 60 days after receipt of the request. If the covered entity is unable to meet the deadline, the covered entity may extend the deadline by no more than 30 days. The covered entity must inform the individual in writing, within the standard 60-day deadline, of the reason for the delay and the date by which the covered entity will provide the request.

A covered entity may only extend the deadline one time per request for accounting.

The NPRM did not address whether a covered entity could charge a fee for the accounting of disclosures.

In the final rule, we provide that individuals have a right to receive one free accounting per 12 month period. For each additional request by an individual within the 12 month period, the covered entity may charge a reasonable, cost-based fee. If it imposes such a fee, the covered entity must inform the individual of the fee in advance and provide the individual with an opportunity to withdraw or modify the request in order to avoid or reduce the fee.

Procedures and Documentation

As in the proposed rule, we establish documentation requirements for covered entities subject to this provision. In accordance with § 164.530(j), for disclosures that are subject to the accounting requirement, the covered entity must retain documentation of the information required to be included in the accounting. The covered entity must also retain a copy of any accounting provided and must document the titles of the persons or offices responsible for receiving and processing requests for an accounting.

Section 164.530—Administrative Requirements

Designation of a Privacy Official and Contact Person

In § 164.518(a) of the NPRM, we proposed that covered entities be required to designate an individual as the covered entity's privacy official, responsible for the implementation and development of the entity's privacy policies and procedures. We also proposed that covered entities be required to designate a contact person to receive complaints about privacy and provide information about the matters covered by the entity's notice. We indicated that the contact person could be, but was not required to be, the person designated as the privacy official. We proposed to leave implementation details to the discretion of the covered entity. We expected implementation to vary widely depending on the size and nature of the covered entity, with small offices assigning this as an additional duty to an existing staff person, and large organizations creating a full-time privacy official. In proposed § 164.512, we also proposed to require the covered plan or provider's privacy notice to include the name of a contact person for privacy matters.

The final regulation retains the requirements for a privacy official and contact person as specified in the NPRM. These designations must be documented. The designation of privacy official and contact person positions within affiliated entities will depend on how the covered entity chooses to designate the covered entity(ies) under § 164.504(b). If a subsidiary is defined as a covered entity under this regulation, then a separate privacy official and contact person is required for that covered entity. If several subsidiaries are designated as a single covered entity, pursuant to § 164.504(b), then together they need have only a single privacy officer and contact person. If several covered entities share a notice for services provided on the same premises, pursuant to § 164.520(d), that notice need designate only one privacy official and contact person for the information collected under that notice.

These requirements are consistent with the approach recommended by the Joint Commission on Accreditation of Healthcare Organizations, and the National Committee for Quality Assurance, in its paper ''Protecting Personal Health Information; A framework for Meeting the Challenges in a Managed Care Environment.'' This paper notes that ''accountability is enhanced by having focal points who are responsible for assessing compliance with policies and procedures * * * '' (p. 29)

Training

In § 164.518(b) of the NPRM we proposed to require that covered entities provide training on the entities' policies and procedures to all members of the workforce likely to have access to protected health information. Each entity would be required to provide initial training by the date on which this rule became applicable. After that date, each covered entity would have to provide training to new members of the workforce within a reasonable time after joining the entity. In addition, we proposed that when a covered entity made material changes in its privacy policies or procedures, it would be required to retrain those members of the workforce whose duties were related to the change within a reasonable time of making the change.

The NPRM would have required that, upon completion of the training, the trainee would be required to sign a statement certifying that he or she received the privacy training and would honor all of the entity's privacy policies and procedures. Entities would determine the most effective means of achieving this training requirement for their workforce. We also proposed that, at least every three years after the initial training, covered entities would be required to have each member of the workforce sign a new statement certifying that he or she would honor all of the entity's privacy policies and procedures. The covered entity would have been required to document its policies and procedures for complying with the training requirements.

The final regulation requires covered entities to train all members of their workforce on the policies and procedures with respect to protected health information required by this rule, as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity. We do not change the proposed time lines for training existing and new members of the workforce, or for training due to material changes in the covered entity's policies and procedures. We eliminate both the requirement for employees to sign a certification following training and the triennial re-certification requirement. Covered entities are responsible for implementing policies and procedures to meet these requirements and for documenting that training has been provided.

Safeguards

In § 164.518(c) of the NPRM, we proposed to require covered entities to put in place administrative, technical, and physical safeguards to protect the privacy of protected health information. We made reference in the preamble to similar requirements proposed for certain electronic information in the Notice of Proposed Rulemaking entitled the Security and Electronic Signature Standards (HCFA–0049–P). We stated that we were proposing parallel and consistent requirements for safeguarding the privacy of protected health information. In § 164.518(c)(3) of the NPRM, we required covered entities to have safeguards to ensure that information was not used in violation of the requirements of this subpart or by people who did not have proper authorization to access the information.

We do not change the basic proposed requirements that covered entities have administrative, technical and physical safeguards to protect the privacy of protected health information. We combine the proposed requirements into a single standard that requires covered entities to safeguard protected health information from accidental or intentional use or disclosure that is a violation of the requirements of this rule

and to protect against the inadvertent disclosure of protected health information to persons other than the intended recipient. Limitations on access to protected health information by the covered entities workforce will also be covered by the policies and procedures for ''minimum necessary'' use of protected health information, pursuant to § 164.514(d). We expect these provisions to work in tandem.

We do not prescribe the particular measures that covered entities must take to meet this standard, because the nature of the required policies and procedures will vary with the size of the covered entity and the type of activities that the covered entity undertakes. (That is, as with other provisions of this rule, this requirement is ''scalable.'') Examples of appropriate safeguards include requiring that documents containing protected health information be shredded prior to disposal, and requiring that doors to medical records departments (or to file cabinets housing such records) remain locked and limiting which personnel are authorized to have the key or pass-code. We intend this to be a common sense, scalable, standard. We do not require covered entities to guarantee the safety of protected health information against all assaults. Theft of protected health information may or may not signal a violation of this rule, depending on the circumstances and whether the covered entity had reasonable policies to protect against theft. Organizations such as the Association for Testing and Materials (ASTM) and the American Health Information Management Association (AHIMA) have developed a body of recommended practices for handling of protected health information that covered entities may find useful.

We note that the proposed HIPAA Security Standards would require covered entities to safeguard the privacy and integrity of health information. For electronic information, compliance with both regulations will be required.

In § 164.518(c)(2) of the NPRM we proposed requirements for verification procedures to establish identity and authority for permitted disclosures of protected health information.

In the final rule, this material has been moved to § 164.514(h).

Use or Disclosure of Protected Health Information by Whistleblowers

In § 164.518(c)(4) of the NPRM, this provision was entitled ''Implementation Specification: Disclosures by whistleblowers.'' It is now retitled ''Disclosures by whistleblowers,'' with certain changes, and moved to § 164.502(j)(1).

Complaints to the Covered Entity

In § 164.518(d) of the NPRM, we proposed to require covered entities to have a mechanism for receiving complaints from individuals regarding the health plan's or provider's compliance with the requirements of this proposed rule. We did not require that the health plan or provider develop a formal appeals mechanism, nor that ''due process'' or any similar standard be applied. Additionally, there was no requirement to respond in any particular manner or time frame.

We proposed two basic requirements for the complaint process. First, the covered health plan or health care provider would be required to identify in the notice of information practices a contact person or office for receiving complaints. Second, the health plan or provider would be required to maintain a record of the complaints that are filed and a brief explanation of their resolution, if any.

In the final rule, we retain the requirement for an internal complaint process for compliance with this rule, including the two basic requirements of identifying a contact person and documenting complaints received and their dispositions, if any. We expand the scope of complaints that covered entities must have a means of receiving to include complaints concerning violations of the covered entity's privacy practices, not just violations of the rule. For example, a covered entity must have a mechanism for receiving a complaint that patient information is used at a nursing station in a way that it can also be viewed by visitors to the hospital, regardless of whether the practices at the nursing stations might constitute a violation of this rule.

Sanctions

In § 164.518(e) of the NPRM, we proposed to require all covered entities to develop, and apply when appropriate, sanctions against members of its workforce who failed to comply with privacy policies or procedures of the covered entity or with the requirements of the rule. Covered entities would be required to develop and impose sanctions appropriate to the nature of the violation. The preamble stated that the type of sanction applied would vary depending on factors such as the severity of the violation, whether the violation was intentional or unintentional, and whether the violation indicated a pattern or practice of improper use or disclosure of protected health information. Sanctions could range from a warning to termination. The NPRM preamble language also stated that covered entities would be required to apply sanctions against business associates that violated the proposed rule.

In the final rule, we retain the requirement for sanctions against members of a covered entity's workforce. We also require a covered entity to have written policies and procedures for the application of appropriate sanctions for violations of this subpart and to document those sanctions. These sanctions do not apply to whistleblower activities that meet the provisions of § 164.502(j) or complaints, investigations, or opposition that meet the provisions of § 164.530(g)(2). We eliminate language regarding business associates from this section. Requirements with respect to business associates are stated in § 164.504.

Duty To Mitigate

In proposed § 164.518(f), we would have required covered entities to have policies and procedures for mitigating, to the extent practicable, any deleterious effect of a use or disclosure of protected health information in violation of the requirements of this subpart. The NPRM preamble also included specific language applying this requirement to harm caused by members of the covered entity's workforce and business associates.

With respect to business associates, the NPRM preamble but not the NPRM rule text, stated that covered entities would have a duty to take reasonable steps in response to breaches of contract terms. Covered entities generally would not be required to monitor the activities of their business associates, but would be required to take steps to address problems of which they become aware, and, where the breach was serious or repeated, would also be required to monitor the business associate's performance to ensure that the wrongful behavior had been remedied. Termination of the arrangement would be required only if it became clear that a business associate could not be relied upon to maintain the privacy of protected health information provided to it.

In the final rule, we clarify this requirement by imposing a duty for covered entities to mitigate any harmful effect of a use or disclosure of protected health information that is known to the covered entity. We apply the duty to mitigate to a violation of the covered entity's policies and procedures, not just a violation of the requirements of the subpart. We resolve the ambiguities in the NPRM by imposing this duty on covered entities for harm caused by

either members of their workforce or by their business associates.

We eliminate the language regarding potential breaches of business associate contracts from this section. All other requirements with respect to business associates are stated in § 164.504.

Refraining from Intimidating or Retaliatory Acts

In § 164.522(d)(4) of the NPRM, in the Compliance and Enforcement section, we proposed that one of the responsibilities of a covered entity would be to refrain from intimidating or retaliatory acts. Specifically, the rule provided that ''[a] covered entity may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the filing of a complaint under this section, for testifying, assisting, participating in any manner in an investigation, compliance review, proceeding or hearing under this Act, or opposing any act or practice made unlawful by this subpart.''

In the final rule, we continue to require that entities refrain from intimidating or retaliatory acts; however, the provisions have been moved to the Administrative Requirements provisions in § 164.530. This change is not just clerical; in making this change, we apply this provision to the privacy rule alone rather than to all the HIPAA administrative simplification rules. (The compliance and enforcement provisions that were in § 164 are now in Part 160, Subpart C.)

We continue to prohibit retaliation against individuals for filing a complaint with the Secretary, but also prohibit retaliation against any other person who files such a complaint. This is the case because the term ''individual'' is generally limited to the person who is the subject of the information. The final rule prohibits retaliation against persons, not just individuals, for testifying, assisting, or participating in an investigation, compliance review, proceeding or hearing under Part C of Title XI. The proposed regulation referenced the ''Act,'' which is defined in Part 160 as the Social Security Act. Because we only intend to protect activities such as participation in investigations and hearings under the Administrative Simplification provisions of HIPAA, the final rule references Part C of Title XI of the Social Security Act.

The proposed rule would have prohibited retaliatory actions against individuals for opposing any act or practice made unlawful by this subpart. The final rule retains this provision, but applies it to any person, only if the person ''has a good faith belief that the practice opposed is unlawful, the manner of the opposition is reasonable and does not involve a disclosure of protected health information in violation of this subpart.'' The final rule provides additional protections, which had been included in the preamble to the proposed rule. Specifically, we prohibit retaliatory actions against individuals who exercise any right, or participate in any process established by the privacy rule (Part 164 Subpart E), and include as an example the filing of a complaint with the covered entity.

Waiver of Rights

In the final regulation, but not in the proposed regulation, we provide that a covered entity may not require individuals to waive their rights to file a complaint with the Secretary or their other rights under this rule as a condition of the provision of treatment, payment, enrollment in a health plan or eligibility for benefits. This provision ensures that covered entities do not take away the rights that individuals have been provided in Parts 160 and 164.

Requirements for Policies and Procedures, and Documentation Requirements

In § 164.520 of the NPRM, we proposed to require covered entities to develop and document their policies and procedures for implementing the requirements of the rule. In the final regulation we retain this approach, but specify which standards must be documented in each of the relevant sections. In this section, we state the general administrative requirements applicable to all policies and procedures required throughout the regulation.

In § 164.530(i), (j), and (k) of the final rule, we amend the NPRM language in several respects. In § 164.530(i) we require that the policies and procedures be reasonably designed to comply with the standards, implementation specifications, and other requirements of the relevant part of the regulation, taking into account the size of the covered entity and the nature of the activities undertaken by the covered entity that relate to protected health information. However, we clarify that the requirements that policies and procedures be reasonably designed may not be interpreted to permit or excuse any action that violates the privacy regulation. Where the covered entity has stated in its notice that it reserves the right to change information practices, we allow the new practice to apply to information created or collected prior to the effective date of the new practice and establish requirements for making this change. We also establish the conditions for making changes if the covered entity has not reserved the right to change its practices.

We require covered entities to modify in a prompt manner their policies and procedures to comply with changes in relevant law and, where the change also affects the practices stated in the notice, to change the notice. We make clear that nothing in our requirements regarding changes to policies and procedures or changes to the notice may be used by a covered entity to excuse a failure to comply with applicable law.

In § 164.530(j), we require that the policies and procedures required throughout the regulation be maintained in writing, and that any other communication, action, activity, or designation that must be documented under this regulation be documented in writing. We note that ''writing'' includes electronic storage; paper records are not required. We also note that, if a covered entity is required to document the title of a person, we mean the job title or similar description of the relevant position or office.

We require covered entities to retain any documentation required under this rule for at least six years (the statute of limitations period for the civil penalties) from the date of the creation of the documentation, or the date when the document was last in effect, which ever is later. This generalizes the NPRM provision to cover all documentation required under the rule. The language on ''last was in effect'' is a change from the NPRM which was worded ''unless a longer period applies under this subpart.''

This approach is consistent with the approach recommended by the Joint Commission on Accreditation of Healthcare Organizations, and the National Committee for Quality Assurance, in its paper ''Protecting Personal Health Information; A framework for Meeting the Challenges in a Managed Care Environment.'' This paper notes that ''MCOs [Managed Care Organizations] should have clearly defined policies and procedures for dealing with confidentiality issues.'' (p. 29).

Standards for Certain Group Health Plans

We add a new provision (§ 164.530(k)) to clarify the administrative responsibilities of group health plans that offer benefits through issuers and HMOs. Specifically, a group health plan that provides benefits solely through an issuer or HMO, and that does not create, receive or maintain protected health

information other than summary health information or information regarding enrollment and disenrollment, is not subject to the requirements of this section regarding designation of a privacy official and contact person, workforce training, safeguards, complaints, mitigation, or policies and procedures. Such a group health plan is only subject to the requirements of this section regarding documentation with respect to its plan documents. Issuers and HMOs are covered entities under this rule, and thus have independent obligations to comply with this section with respect to the protected health information they maintain about the enrollees in such group health plans. The group health plans subject to this provision will have only limited protected health information. Therefore, imposing these requirements on the group health plan would impose burdens not outweighed by a corresponding enhancement in privacy protections.

Section 164.532—Transition Provisions

In the NPRM, we did not address the effect of the regulation on consents and authorizations covered entities obtained prior to the compliance date of the regulation.

In the final rule, we clarify that, in certain circumstances, a covered entity may continue to rely upon consents, authorizations, or other express legal permissions obtained prior to the compliance date of this regulation to use or disclose protected health information even if these consents, authorizations, or permissions do not meet the requirements set forth in §§ 164.506 or 164.508.

We realize that a covered entity may wish to rely upon a consent, authorization, or other express legal permission obtained from an individual prior to the compliance date of this regulation which permits the use or disclosure of individually identifiable health information for activities that come within treatment, payment, or health care operations (as defined in § 164.501), but that do not meet the requirements for consents set forth in § 164.506. In the final rule, we permit a covered entity to rely upon such consent, authorization, or permission to use or disclose protected health information that it created or received before the applicable compliance date of the regulation to carry out the treatment, payment, or health care operations as long as it meets two requirements. First, the covered entity may not make any use or disclosure that is expressly excluded from the consent, authorization, or permission. Second, the covered entity must comply with all limitations expressed in the consent, authorization, or permission. Thus, we do not require a covered entity to obtain a consent that meets the requirements of § 164.506 to use or disclose this previously obtained protected health information as long as the use or disclosure is consistent with the requirements of this section. However, a covered entity will need to obtain a consent that meets the requirements of § 164.506 to the extent that it is required to obtain a consent under § 164.506 from an individual before it may use or disclose any protected health information it creates or receives after the date by which it must comply with this rule.

Similarly, we recognize that a covered entity may wish to rely upon a consent, authorization, or other express legal permission obtained from an individual prior to the applicable compliance date of this regulation that specifically permits the covered entity to use or disclose individually identifiable health information for activities other than to carry out treatment, payment, or health care operations. In the final rule, we permit a covered entity to rely upon such a consent, authorization, or permission to use or disclose protected health information that it created or received before the applicable compliance date of the regulation for the specific activities described in the consent, authorization, or permission as long as the covered entity complies with two requirements. First, the covered entity may not make any use or disclosure that is expressly excluded from the consent, authorization, or permission. Second, the covered entity must comply with all limitations expressed in the consent, authorization, or permission. Thus, we do not required a covered entity to obtain an authorization that meets the requirements of § 164.508 to use or disclose this previously obtained protected health information so long as the use or disclosure is consistent with the requirements of this section. However, a covered entity will need to obtain an authorization that meets the requirements of § 164.508, to the extent that it is required to obtain an authorization under this rule, from an individual before it may use or disclose any protected health information it creates or receives after the date by which it must comply with this rule.

Additionally, the final rule acknowledges that covered entities may wish to rely upon consents, authorizations, or other express legal permission obtained from an individual prior to the applicable compliance date for a specific research project that includes the treatment of individuals, such as clinical trials. These consents, authorizations, or permissions may specifically permit a use or disclosure of individually identifiable health information for purposes of the project. Alternatively, they may be general consents to participate in the project. A covered entity may use or disclose protected health information it created or received before or after to the applicable compliance date of this rule for purposes of the project provided that the covered entity complies with all limitations expressed in the consent, authorization, or permission.

If, pursuant to this section, a covered entity relies upon a previously obtained consent, authorization, or other express legal permission and agrees to a request for a restriction by an individual under § 164.522(a), any subsequent use or disclosure under that consent, authorization, or permission must comply with the agreed upon restriction as well.

We believe it is necessary to grandfather in previously obtained consents, authorizations, or other express legal permissions in these circumstances to ensure that important functions of the health care system are not impeded. We link the effectiveness of such consents, authorizations, or permissions in these circumstances to the applicable compliance date to give covered entities sufficient notice of the requirements set forth in §§ 164.506 and 164.508.

The rule does not change the past effectiveness of consents, authorizations, or other express legal permissions that do not come within this section. This means that uses or disclosures of individually identifiable health information made prior to the compliance date of this regulation are not subject to sanctions, even if they were made pursuant to documents or permissions that do not meet the requirements of this rule or were made without permission. This rule alters only the future effectiveness of the previously obtained consents, authorizations, or permissions. Covered entities are not required to rely upon these consents, authorizations, or permissions and may obtain new consents or authorizations that meet the applicable requirements of §§ 164.506 and 164.508.

When reaching this decision, we considered requiring all covered entities to obtain new consents or authorizations consistent with the requirements of §§ 164.506 and 164.508 before they would be able to use or disclose protected health information obtained

after the compliance date of these rules. We rejected this option because we recognize that covered entities may not always be able to obtain new consents or authorizations consistent with the requirements of §§ 164.506 and 164.508 from all individuals upon whose information they rely. We also refrained from impeding the rights of covered entities to exercise their interests in the records they have created. We do not require covered entities with existing records or databases to destroy or remove the protected health information for which they do not have valid consents or authorizations that meet the requirements of §§ 164.506 and 164.508. Covered entities may rely upon the consents, authorizations, or permissions they obtained from individuals prior to the applicable compliance date of this regulation consistent with the constraints of those documents and the requirements discussed above.

We note that if a covered entity obtains before the applicable compliance date of this regulation a consent that meets the requirements of § 164.506, an authorization that meets the requirements of § 164.508, or an IRB or privacy board waiver of authorization that meets the requirements of § 164.512(i), the consent, authorization, or waiver is effective for uses or disclosures that occur after the compliance date and that are consistent with the terms of the consent, authorization, or waiver.

Section 164.534—Compliance Dates for Initial Implementation of the Privacy Standards

In the NPRM, we provided that a covered entity must be in compliance with this subpart not later than 24 months following the effective date of this rule, except that a covered entity that is a small health plan must be in compliance with this subpart not later than 36 months following the effective date of the rule.

The final rule did not make any substantive changes. The format is changed so as to more clearly present the various compliance dates. The final rule lists the types of covered entities and then the various dates that would apply to each of these entities.

III. Section-by-Section Discussion of Comments

The following describes the provisions in the final regulation, and the changes we make to the proposed provisions section-by-section. Following each section are our responses to the comments to that section. This section of the preamble is organized to follow the corresponding section of the final rule, not the NPRM.

General Comments

We received many comments on the rule overall, not to a particular provision. We respond to those comments here. Similar comments, but directed to a specific provision in the proposed rule, are answered below in the corresponding section of this preamble.

Comments on the Need for Privacy Standards, and Effects of this Regulation on Current Protections

Comment: Many commenters expressed the opinion that federal legislation is necessary to protect the privacy of individuals' health information. One comment advocated Congressional efforts to provide a comprehensive federal health privacy law that would integrate the substance abuse regulations with the privacy regulation.

Response: We agree that comprehensive privacy legislation is urgently needed. This administration has urged the Congress to pass such legislation. While this regulation will improve the privacy of individuals' health information, only legislation can provide the full array of privacy protection that individuals need and deserve.

Comment: Many commenters noted that they do not go to a physician, or do not completely share health information with their physician, because they are concerned about who will have access to that information. Many physicians commented on their patients' reluctance to share information because of fear that their information will later be used against them.

Response: We agree that strong federal privacy protections are necessary to enhance patients' trust in the health care system.

Comment: Many commenters expressed concerns that this regulation will allow access to health information by those who today do not have such access, or would allow their physician to disclose information which may not lawfully be disclosed today. Many of these commenters stated that today, they consent to every disclosure of health information about them, and that absent their consent the privacy of their health information is ''absolute.'' Others stated that, today, health information is disclosed only pursuant to a judicial order. Several commenters were concerned that this regulation would override stronger state privacy protection.

Response: This regulation does not, and cannot, reduce current privacy protections. The statutory language of the HIPAA specifically mandates that this regulation does not preempt state laws that are more protective of privacy.

As discussed in more detail in later this preamble, while many people believe that they must be asked permission prior to any release of health information about them, current laws generally do not impose such a requirement. Similarly, as discussed in more detail later in this preamble, judicial review is required today only for a small proportion of releases of health information.

Comment: Many commenters asserted that today, medical records ''belong'' to patients. Others asserted that patients own their medical information and health care providers and insurance companies who maintain health records should be viewed as custodians of the patients' property.

Response: We do not intend to change current law regarding ownership of or responsibility for medical records. In developing this rule we reviewed current law on this and related issues, and built on that foundation.

Under state laws, medical records are often the property of the health care provider or medical facility that created them. Some state laws also provide patients with access to medical records or an ownership interest in the health information in medical records. However, these laws do not divest the health care provider or the medical facility of its ownership interest in medical records. These statutes typically provide a patient the right to inspect or copy health information from the medical record, but not the right to take the provider's original copy of an item in the medical record. If a particular state law provides greater ownership rights, this regulation leaves such rights in place.

Comment: Some commenters argued that the use and disclosure of sensitive personal information must be strictly regulated, and violation of such regulations should subject an entity to significant penalties and sanctions.

Response: We agree, and share the commenters' concern that the penalties in the HIPAA statute are not sufficient to fully protect individuals' privacy interests. The need for stronger penalties is among the reasons we believe Congress should pass comprehensive privacy legislation.

Comment: Many commenters expressed the opinion that the proposed ruled should provide stricter privacy protections.

Response: We received nearly 52,000 comments on the proposed regulation, and make substantial changes to the proposal in response to those comments. Many of these changes will strengthen the protections that were proposed in the NPRM.

Comment: Many comments express concerns that their health information will be given to their employers.

Response: We agree that employer access to health information is a particular concern. In this final regulation, we make significant changes to the NPRM that clarify and provide additional safeguards governing when and how the health plans covered by this regulation may disclose health information to employers.

Comment: Several commenters argued that individuals should be able to sue for breach of privacy.

Response: We agree, but do not have the legislative authority to grant a private right of action to sue under this statute. Only Congress can grant that right.

Objections to Government Access to Protected Health Information

Comment: Many commenters urged the Department not to create a government database of health information, or a tracking system that would enable the government to track individuals health information.

Response: This regulation does not create such a database or tracking system, nor does it enable future creation of such a database. This regulation describes the ways in which health plans, health care clearinghouses, and certain health care providers may use and disclose identifiable health information with and without the individual's consent.

Comment: Many commenters objected to government access to or control over their health information, which they believe the proposed regulation would provide.

Response: This regulation does not increase current government access to health information. This rule sets minimum privacy standards. It does not require disclosure of health information, other than to the subject of the records or for enforcement of this rule. Health plans and health care providers are free to use their own professional ethics and judgement to adopt stricter policies for disclosing health information.

Comment: Some commenters viewed the NPRM as creating fewer hurdles for government access to protected health information than for access to protected health information by private organizations. Some health care providers commented that the NPRM would impose substantial new restrictions on private sector use and disclosure of protected health information, but would make government access to protected health information easy. One consumer advocacy group made the same observation.

Response: We acknowledge that many of the national priority purposes for which we allow disclosure of protected health information without consent or authorization are for government functions, and that many of the governmental recipients of such information are not governed by this rule. It is the role of government to undertake functions in the broader public interest, such as public health activities, law enforcement, identification of deceased individuals through coroners' offices, and military activities. It is these public purposes which can sometimes outweigh an individual's privacy interest. In this rule, we specify the circumstances in which that balance is tipped toward the public interest with respect to health information. We discuss the rationale behind each of these permitted disclosures in the relevant preamble sections below.

Miscellaneous Comments

Comment: Many commenters objected to the establishment of a unique identifier for health care or other purposes.

Response: This regulation does not create an identifier. We assume these comments refer to the unique health identifier that Congress directed the Secretary to promulgate under section1173(b) of the Social Security Act, added by section 262 of the HIPAA. Because of the public concerns about such an identifier, in the summer of 1998 Vice President Gore announced that the Administration would not promulgate such a regulation until comprehensive medical privacy protections were in place. In the fall of that year, Congress prohibited the Department from promulgating such an identifier, and that prohibition remains in place. The Department has no plans to promulgate a unique health identifier.

Comment: Many commenters asked that we withdraw the proposed regulation and not publish a final rule.

Response: Under section 264 of the HIPAA, the Secretary is required by Congress to promulgate a regulation establishing standards for health information privacy. Further, for the reasons explained throughout this preamble above, we believe that the need to protect health information privacy is urgent and that this regulation is in the public's interest.

Comment: Many commenters express the opinion that their consent should be required for all disclosure of their health information.

Response: We agree that consent should be required prior to release of health information for many purposes, and impose such a requirement in this regulation. Requiring consent prior to all release of health information, however, would unduly jeopardize public safety and make many operations of the health care system impossible. For example, requiring consent prior to release of health information to a public health official who is attempting to track the source of an outbreak or epidemic could endanger thousands of lives. Similarly, requiring consent before an oversight official could audit a health plan would make detection of health care fraud all but impossible; it could take health plans months or years to locate and obtain the consent of all current and past enrollees, and the health plan would not have a strong incentive to do so. These uses of medical information are clearly in the public interest.

In this regulation, we must balance individuals' privacy interests against the legitimate public interests in certain uses of health information. Where there is an important public interest, this regulation imposes procedural safeguards that must be met prior to release of health information, in lieu of a requirement for consent. In some instances the procedural safeguards consist of limits on the circumstances in which information may be disclosed, in others the safeguards consist of limits on what information may be disclosed, and in other cases we require some form of legal process (*e.g.,* a warrant or subpoena) prior to release of health information. We also allow disclosure of health information without consent where other law mandates the disclosures. Where such other law exists, another public entity has made the determination that the public interests outweigh the individual's privacy interests, and we do not upset that determination in this regulation. In short, we tailor the safeguards to match the specific nature of the public purpose. The specific safeguards are explained in each section of this regulation below.

Comment: Many comments address matters not relevant to this regulation, such as alternative fuels, hospital reimbursement, and gulf war syndrome.

Response: These and similar matters are not relevant to this regulation and will not be addressed further.

Comment: A few commenters questioned why this level of detail is needed in response to the HIPAA Congressional mandate.

Response: This level of detail is necessary to ensure that individuals' rights with respect to their health information are clear, while also ensuring that information necessary for important public functions, such as protecting public health, promoting biomedical research, fighting health care fraud, and notifying family members in disaster situations, will not be impaired by this regulation. We designed this rule to reflect current practices and change some of them. The comments and our fact finding revealed the complexity of current health information practices, and we believe that the complexity entailed in reflecting those practices is better public policy than a perhaps simpler rule that disturbed important information flows.

Comment: A few comments stated that the goal of administrative simplification should never override the privacy of individuals.

Response: We believe that privacy is a necessary component of administrative simplification, not a competing interest.

Comment: At least one commenter said that the goal of administrative simplification is not well served by the proposed rule.

Response: Congress recognized that privacy is a necessary component of administrative simplification. The standardization of electronic health information mandated by the HIPAA that make it easier to share that information for legitimate purposes also make the inappropriate sharing of that information easier. For this reason, Congress included a mandate for privacy standards in this section of the HIPAA. Without appropriate privacy protections, public fear and instances of abuse would make it impossible for us to take full advantage of the administrative and costs benefits inherent in the administrative simplification standards.

Comment: At least one commenter asked us to require psychotherapists to assert any applicable legal privilege on patients' behalf when protected health information is requested.

Response: Whether and when to assert a claim of privilege on a patient's behalf is a matter for other law and for the ethics of the individual health care provider. This is not a decision that can or should be made by the federal government.

Comment: One commenter called for HHS to consider the privacy regulation in conjunction with the other HIPAA standards. In particular, this comment focused on the belief that the Security Standards should be compatible with the existing and emerging health care and information technology industry standards.

Response: We agree that both this regulation and the final Security Regulation should be compatible with existing and emerging technology industry standards. This regulation is ''technology neutral.'' We do not mandate the use of any particular technologies, but rather set standards which can be met through a variety of means.

Comment: Several commenters claimed that the statutory authority given under HIPAA cannot provide meaningful privacy protections because many entities with access to protected health information, such as employers, worker's compensation carriers, and life insurance companies, are not covered entities. These commenters expressed support for comprehensive legislation to close many of the existing loopholes.

Response: We agree with the commenters that comprehensive legislation is necessary to provide full privacy protection and have called for members of Congress to pass such legislation to prevent unauthorized and potentially harmful uses and disclosures of information.

Part 160—Subpart A—General Provisions

Section 160.103—Definitions

Business Associate

The response to comments on the definition of ''business partner,'' renamed in this rule as ''business associate,'' is included in the response to comments on the requirements for business associates in the preamble discussion of § 164.504.

Covered Entity

Comment: A number of commenters urged the Department to expand or clarify the definition of ''covered entity'' to include certain entities other than health care clearinghouses, health plans, and health care providers who conduct standard transactions. For example, several commenters asked that the Department generally expand the scope of the rule to cover all entities that receive or maintain individually identifiable health information; others specifically urged the Department to cover employers, marketing firms, and legal entities that have access to individually identifiable health information. Some commenters asked that life insurance and casualty insurance carriers be considered covered entities for purposes of this rule. One commenter recommended that Pharmacy Benefit Management (PBM) companies be considered covered entities so that they may use and disclose protected health information without authorization.

In addition, a few commenters asked the Department to clarify that the definition includes providers who do not directly conduct electronic transactions if another entity, such as a billing service or hospital, does so on their behalf.

Response: We understand that many entities may use and disclose individually identifiable health information. However, our jurisdiction under the statute is limited to health plans, health care clearinghouses, and health care providers who transmit any health information electronically in connection with any of the standard financial or administrative transactions in section 1173(a) of the Act. These are the entities referred to in section 1173(a)(1) of the Act and thus listed in § 160.103 of the final rule. Consequently, once protected health information leaves the purview of one of these covered entities, their business associates, or other related entities (such as plan sponsors), the information is no longer afforded protection under this rule. We again highlight the need for comprehensive federal legislation to eliminate such gaps in privacy protection.

We also provide the following clarifications with regard to specific entities.

We clarify that employers and marketing firms are not covered entities. However, employers may be plan sponsors of a group health plan that is a covered entity under the rule. In such a case, specific requirements apply to the group health plan. See the preamble on § 164.504 for a discussion of specific ''firewall'' and other organizational requirements for group health plans and their employer sponsors. The final rule also contains provisions addressing when an insurance issuer providing benefits under a group health plan may disclose summary health information to a plan sponsor.

With regard to life and casualty insurers, we understand that such benefit providers may use and disclose individually identifiable health information. However, Congress did not include life insurers and casualty insurance carriers as ''health plans'' for the purposes of this rule and therefore they are not covered entities. See the discussion regarding the definition of ''health plan'' and excepted benefits.

In addition, we clarify that a PBM is a covered entity only to the extent that it meets the definition of one or more of the entities listed in § 160.102. When providing services to patients through managed care networks, it is likely that a PBM is acting as a business associate of a health plan, and may thus use and disclose protected health information pursuant to the relevant provisions of this rule. PBMs may also be business associates of health care providers. See the preamble sections on §§ 164.502, 164.504, and 164.506 for discussions of the specific requirements related to business associates and consent.

Lastly, we clarify that health care providers who do not submit HIPAA transactions in standard form become covered by this rule when other entities, such as a billing service or a hospital, transmit standard electronic transactions on their behalf. The provider could not circumvent these requirements by assigning the task to a contractor.

Comment: Many commenters urged the Department to restrict or clarify the definition of ''covered entity'' to exclude certain entities, such as department-operated hospitals (public hospitals); state Crime Victim Compensation Programs; employers; and certain lines of insurers, such as workers' compensation insurers, property and casualty insurers, reinsurers, and stop-loss insurers. One commenter expressed concern that clergy, religious practitioners, and other faith-based service providers would have to abide by the rule and asked that the Department exempt prayer healing and non-medical health care.

Response: The Secretary provides the following clarifications in response to these comments. To the extent that a ''department-operated hospital'' meets the definition of a ''health care provider'' and conducts any of the standard transactions, it is a covered entity for the purposes of this rule. We agree that a state Crime Victim Compensation Program is not a covered entity if it is not a health care provider that conducts standard transactions, health plan, or health care clearinghouse. Further, as described above, employers are not covered entities.

In addition, we agree that workers' compensation insurers, property and casualty insurers, reinsurers, and stop-loss insurers are not covered entities, as they do not meet the statutory definition of ''health plan.'' See further discussion in the preamble on § 160.103 regarding the definition of ''health plan.'' However, activities related to ceding, securing, or placing a contract for reinsurance, including stop-loss insurance, are health care operations in the final rule. As such, reinsurers and stop-loss insurers may obtain protected health information from covered entities.

Also, in response to the comment regarding religious practitioners, the Department clarifies that ''health care'' as defined under the rule does not include methods of healing that are solely spiritual. Therefore, clergy or other religious practitioners that provide solely religious healing services are not health care providers within the meaning of this rule, and consequently not covered entities for the purposes of this rule.

Comment: A few commenters expressed general uncertainty and requested clarification as to whether certain entities were covered entities for the purposes of this rule. One commenter was uncertain as to whether the rule applies to certain social service entities, in addition to clinical social workers that the commenter believes are providers. Other commenters asked whether researchers or non-governmental entities that collect and analyze patient data to monitor and evaluate quality of care are covered entities. Another commenter requested clarification regarding the definition's application to public health agencies that also are health care providers as well as how the rule affects public health agencies in their data collection from covered entities.

Response: Whether the professionals described in these comments are covered by this rule depends on the activities they undertake, not on their profession or degree. The definitions in this rule are based on activities and functions, not titles. For example, a social service worker whose activities meet this rule's definition of health care will be a health care provider. If that social service worker also transmits information in a standard HIPAA transaction, he or she will be a covered health entity under this rule. Another social service worker may provide services that do not meet the rule's definition of health care, or may not transmit information in a standard transaction. Such a social service worker is not a covered entity under this rule. Similarly, researchers in and of themselves are not covered entities. However, researchers may also be health care providers if they provide health care. In such cases, the persons, or entities in their role as health care providers may be covered entities if they conduct standard transactions.

With regard to public health agencies that are also health care providers, the health care provider ''component'' of the agency is the covered entity if that component conducts standard transactions. See discussion of ''health care components'' below. As to the data collection activities of a public health agency, the final rule in § 164.512(b) permits a covered entity to disclose protected health information to public health authorities under specified circumstances, and permits public health agencies that are also covered entities to use protected health information for these purposes. See § 164.512(b) for further details.

Comment: A few commenters requested that the Department clarify that device manufacturers are not covered entities. They stated that the proposal did not provide enough guidance in cases where the ''manufacturer supplier'' has only one part of its business that acts as the ''supplier,'' and additional detail is needed about the relationship of the ''supplier component'' of the company to the rest of the business. Similarly, another commenter asserted that drug, biologics, and device manufacturers should not be covered entities simply by virtue of their manufacturing activities.

Response: We clarify that if a supplier manufacturer is a Medicare supplier, then it is a health care provider, and it is a covered entity if it conducts standard transactions. Further, we clarify that a manufacturer of supplies related to the health of a particular individual, e.g., prosthetic devices, is a health care provider because the manufacturer is providing ''health care'' as defined in the rule. However, that manufacturer is a covered entity only if it conducts standard transactions. We do not intend that a manufacturer of supplies that are generic and not customized or otherwise specifically designed for particular individuals, e.g., ace bandages for a hospital, is a health care provider. Such a manufacturer is not providing ''health care'' as defined in the rule and is therefore not a covered entity. We note that, even if such a manufacturer is a covered entity, it may be an ''indirect treatment provider'' under this rule, and thus not subject to all of the rule's requirements.

With regard to a ''supplier component,'' the final rule addresses the status of the unit or unit(s) of a larger entity that constitute a ''health care component.'' See further discussion under § 164.504 of this preamble.

Finally, we clarify that drug, biologics, and device manufacturers are not health care providers simply by virtue of their manufacturing activities. The manufacturer must be providing health care consistent with the final

rule's definition in order to be considered a health care provider.

Comment: A few commenters asked that the Department clarify that pharmaceutical manufacturers are not covered entities. It was explained that pharmaceutical manufacturers provide support and guidance to doctors and patients with respect to the proper use of their products, provide free products for doctors to distribute to patients, and operate charitable programs that provide pharmaceutical drugs to patients who cannot afford to buy the drugs they need.

Response: A pharmaceutical manufacturer is only a covered entity if the manufacturer provides ''health care'' according to the rule's definition and conducts standard transactions. In the above case, a pharmaceutical manufacturer that provides support and guidance to doctors and patients regarding the proper use of their products is providing ''health care'' for the purposes of this rule, and therefore, is a health care provider to the extent that it provides such services. The pharmaceutical manufacturer that is a health care provider is only a covered entity, however, if it conducts standard transactions. We note that this rule permits a covered entity to disclose protected health information to any person for treatment purposes, without specific authorization from the individual. Therefore, a covered health care provider is permitted to disclose protected health information to a pharmaceutical manufacturer for treatment purposes. Providing free samples to a health care provider does not in itself constitute health care. For further analysis of pharmacy assistance programs, see response to comment on § 164.501, definition of ''payment.''

Comment: Several commenters asked about the definition of ''covered entity'' and its application to health care entities within larger organizations.

Response: A detailed discussion of the final rule's organizational requirements and firewall restrictions for ''health care components'' of larger entities, as well as for affiliated, and other entities is found at the discussion of § 164.504 of this preamble. The following responses to comments provide additional information with respect to particular ''component entity'' circumstances.

Comment: Several commenters asked that we clarify the definition of covered entity to state that with respect to persons or organizations that provide health care or have created health plans but are primarily engaged in other unrelated businesses, the term ''covered entity'' encompasses only the health care components of the entity. Similarly, others recommended that only the component of a government agency that is a provider, health plan, or clearinghouse should be considered a covered entity.

Other commenters requested that we revise proposed § 160.102 to apply only to the component of an entity that engages in the transactions specified in the rule. Commenters stated that companies should remain free to employ licensed health care providers and to enter into corporate relationships with provider institutions without fear of being considered to be a covered entity. Another commenter suggested that the regulation not apply to the provider-employee or employer when neither the provider nor the company are a covered entity.

Some commenters specifically argued that the definition of ''covered entity'' did not contemplate an integrated health care system and one commenter stated that the proposal would disrupt the multi-disciplinary, collaborative approach that many take to health care today by treating all components as separate entities. Commenters, therefore, recommended that the rule treat the integrated entity, not its constituent parts, as the covered entity.

A few commenters asked that the Department further clarify the definition with respect to the unique organizational models and relationships of academic medical centers and their parent universities and the rules that govern information exchange within the institution. One commenter asked whether faculty physicians who are paid by a medical school or faculty practice plan and who are on the medical staff of, but not paid directly by, a hospital are included within the covered entity. Another commenter stated that it appears that only the health center at an academic institution is the covered entity. Uncertainty was also expressed as to whether other components of the institution that might create protected health information only incidentally through the conduct of research would also be covered.

Response: The Department understands that in today's health care industry, the relationships among health care entities and non-health care organizations are highly complex and varied. Accordingly, the final rule gives covered entities some flexibility to segregate or aggregate its operations for purposes of the application of this rule. The new component entity provision can be found at §§ 164.504(b)-(c). In response to the request for clarification on whether the rule would apply to a research component of the covered entity, we point out that if the research activities fall outside of the health care component they would not be subject to the rule. One organization may have one or several ''health care component(s)'' that each perform one or more of the health care functions of a covered entity, i.e., health care provider, health plan, health care clearinghouse. In addition, the final rule permits covered entities that are affiliated, *i.e.,* share common ownership or control, to designate themselves, or their health care components, together to be a single covered entity for purposes of the rule.

It appears from the comments that there is not a common understanding of the meaning of ''integrated delivery system.'' Arrangements that apply this label to themselves operate and share information many different ways, and may or may not be financially or clinically integrated. In some cases, multiple entities hold themselves out as one enterprise and engage together in clinical or financial activities. In others, separate entities share information but do not provide treatment together or share financial risk. Many health care providers participate in more than one such arrangement.

Therefore, we do not include a separate category of ''covered entity'' under this rule for ''integrated delivery systems'' but instead accommodate the operations of these varied arrangements through the functional provisions of the rule. For example, covered entities that operate as ''organized health care arrangements'' as defined in this rule may share protected health information for the operation of such arrangement without becoming business associates of one another. Similarly, the regulation does not require a business associate arrangement when protected health information is shared for purposes of providing treatment. The application of this rule to any particular ''integrated system'' will depend on the nature of the common activities the participants in the system perform. When the participants in such an arrangement are ''affiliated'' as defined in this rule, they may consider themselves a single covered entity (see § 164. 504).

The arrangements between academic health centers, faculty practice plans, universities, and hospitals are similarly diverse. We cannot describe a blanket rule that covers all such arrangements. The application of this rule will depend on the purposes for which the participants in such arrangements share protected health information, whether some or all participants are under common ownership or control, and similar matters. We note that physicians who have staff privileges at a covered

hospital do not become part of that hospital covered entity by virtue of having such privileges.

We reject the recommendation to apply the rule only to components of an entity that engage in the transactions. This would omit as covered entities, for example, the health plan components that do not directly engage in the transactions, including components that engage in important health plan functions such as coverage determinations and quality review. Indeed, we do not believe that the statute permits this result with respect to health plans or health care clearinghouses as a matter of negative implication from section 1172(a)(3). We clarify that only a health care provider must conduct transactions to be a covered entity for purposes of this rule.

We also clarify that health care providers (such as doctors or nurses) who work for a larger organization and do not conduct transactions on their own behalf are workforce members of the covered entity, not covered entities themselves.

Comment: A few commenters asked the Department to clarify the definition to provide that a multi-line insurer that sells insurance coverages, some of which do and others which do not meet the definition of ''health plan,'' is not a covered entity with respect to actions taken in connection with coverages that are not ''health plans.''

Response: The final rule clarifies that the requirements below apply only to the organizational unit or units of the organization that are the ''health care component'' of a covered entity, where the ''covered functions'' are not the primary functions of the entity. Therefore, for a multi-line insurer, the ''health care component'' is the insurance line(s) that conduct, or support the conduct of, the health care function of the covered entity. Also, it should be noted that excepted benefits, such as life insurance, are not included in the definition of ''health plan.'' (See preamble discussion of § 164.504).

Comment: A commenter questioned whether the Health Care Financing Administration (HCFA) is a covered entity and how HCFA will share data with Medicare managed care organizations. The commenter also questioned why the regulation must apply to Medicaid since the existing Medicaid statute requires that states have privacy standards in place. It was also requested that the Department provide a definition of ''health plan'' to clarify that state Medicaid Programs are considered as such.

Response: HCFA is a covered entity because it administers Medicare and Medicaid, which are both listed in the statute as health plans. Medicare managed care organizations are also covered entities under this regulation. As noted elsewhere in this preamble, covered entities that jointly administer a health plan, such as Medicare + Choice, are both covered entities, and are not business associates of each other by virtue of such joint administration.

We do not exclude state Medicaid programs. Congress explicitly included the Medicaid program as a covered health plan in the HIPAA statute.

Comment: A commenter asked the Department to provide detailed guidance as to when providers, plans, and clearinghouses become covered entities. The commenter provided the following example: if a provider submits claims only in paper form, and a coordination of benefits (COB) transaction is created due to other insurance coverage, will the original provider need to be notified that the claim is now in electronic form, and that it has become a covered entity? Another commenter voiced concern as to whether physicians who do not conduct electronic transactions would become covered entities if another entity using its records downstream transmits information in connection with a standard transaction on their behalf.

Response: We clarify that health care providers who submit the transactions in standard electronic form, health plans, and health care clearinghouses are covered entities if they meet the respective definitions. Health care providers become subject to the rule if they conduct standard transactions. In the above example, the health care provider would not be a covered entity if the coordination of benefits transaction was generated by a payor.

We also clarify that health care providers who do not submit transactions in standard form become covered by this rule when other entities, such as a billing service or a hospital, transmit standard electronic transactions on the providers' behalf. However, where the downstream transaction is not conducted on behalf of the health care provider, the provider does not become a covered entity due to the downstream transaction.

Comment: Several commenters discussed the relationship between section 1179 of the Act and the privacy regulations. One commenter suggested that HHS retain the statement that a covered entity means ''the entities to which part C of title XI of the Act applies.'' In particular, the commenter observed that section 1179 of the Act provides that part C of title XI of the Act does not apply to financial institutions or to entities acting on behalf of such institutions that are covered by the section 1179 exemption. Thus, under the definition of covered entity, they comment that financial institutions and other entities that come within the scope of the section 1179 exemption are appropriately not covered entities.

Other commenters maintained that section 1179 of the Act means that the Act's privacy requirements do not apply to the request for, or the use or disclosure of, information by a covered entity with respect to payment: (a) For transferring receivables; (b) for auditing; (c) in connection with—(i) a customer dispute; or (ii) an inquiry from or to a customer; (d) in a communication to a customer of the entity regarding the customer's transactions payment card, account, check, or electronic funds transfer; (e) for reporting to consumer reporting agencies; or (f) for complying with: (i) a civil or criminal subpoena; or (ii) a federal or state law regulating the entity. These companies expressed concern that the proposed rule did not include the full text of section 1179 when discussing the list of activities that were exempt from the rule's requirements. Accordingly, they recommended including in the final rule either a full listing of or a reference to section 1179's full list of exemptions. Furthermore, these firms opposed applying the proposed rule's minimum necessary standard for disclosure of protected health information to financial institutions because of section 1179.

These commenters suggest that in light of section 1179, HHS lacks the authority to impose restrictions on financial institutions and other entities when they engage in activities described in that section. One commenter expressed concern that even though proposed § 164.510(i) would have permitted covered entities to disclose certain information to financial institutions for banking and payment processes, it did not state clearly that financial institutions and other entities described in section 1179 are exempt from the rule's requirements.

Response: We interpret section 1179 of the Act to mean that entities engaged in the activities of a financial institution, and those acting on behalf of a financial institution, are not subject to this regulation when they are engaged in authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments for a financial institution. The statutory reference to 12 U.S.C. 3401 indicates that Congress chose to adopt the definition of financial institutions found

in the Right to Financial Privacy Act, which defines financial institutions as any office of a bank, savings bank, card issuer, industrial loan company, trust company, savings association, building and loan, homestead association, cooperative bank, credit union, or consumer finance institution located in the United States or one of its Territories. Thus, when we use the term ''financial institution'' in this regulation, we turn to the definition with which Congress provided us. We interpret this provision to mean that when a financial institution, or its agent on behalf of the financial institution, conducts the activities described in section 1179, the privacy regulation will not govern the activity.

If, however, these activities are performed by a covered entity or by another entity, including a financial institution, on behalf of a covered entity, the activities are subject to this rule. For example, if a bank operates the accounts payable system or other ''back office'' functions for a covered health care provider, that activity is not described in section 1179. In such instances, because the bank would meet the rule's definition of ''business associate,'' the provider must enter into a business associate contract with the bank before disclosing protected health information pursuant to this relationship. However, if the same provider maintains an account through which he/she cashes checks from patients, no business associate contract would be necessary because the bank's activities are not undertaken for or on behalf of the covered entity, and fall within the scope of section 1179. In part to give effect to section 1179, in this rule we do not consider a financial institution to be acting on behalf of a covered entity when it processes consumer-conducted financial transactions by debit, credit or other payment card, clears checks, initiates or processes electronic funds transfers, or conducts any other activity that directly facilitates or effects the transfer of funds for compensation for health care.

We do not agree with the comment that section 1179 of the Act means that the privacy regulation's requirements cannot apply to the activities listed in that section; rather, it means that the entities expressly mentioned, financial institutions (as defined in the Right to Financial Privacy Act), and their agents that engage in the listed activities for the financial institution are not within the scope of the regulation. Nor do we interpret section 1179 to support an exemption for disclosures to financial institutions from the minimum necessary provisions of this regulation.

Comment: One commenter recommended that HHS include a definition of ''entity'' in the final rule because HIPAA did not define it. The commenter explained that in a modern health care environment, the organization acting as the health plan or health care provider may involve many interrelated corporate entities and that this could lead to difficulties in determining what ''entities'' are actually subject to the regulation.

Response: We reject the commenter's suggestion. We believe it is clear in the final rule that the entities subject to the regulation are those listed at § 160.102. However, we acknowledge that how the rule applies to integrated or other complex health systems needs to be addressed; we have done so in § 164.504 and in other provisions, such as those addressing organized health care arrangements.

Comment: The preamble should clarify that self-insured group health and workmen's compensation plans are not covered entities or business partners.

Response: In the preamble to the proposed rule we stated that certain types of insurance entities, such as workers' compensation, would not be covered entities under the rule. We do not change this position in this final rule. The statutory definition of health plan does not include workers' compensation products, and the regulatory definition of the term specifically excludes them. However, HIPAA specifically includes most group health plans within the definition of ''health plan.''

Comment: A health insurance issuer asserted that health insurers and third party administrators are usually required by employers to submit reports describing the volume, amount, payee, basis for services rendered, types of claims paid and services for which payment was requested on behalf of it covered employees. They recommended that the rule permit the disclosure of protected health information for such purposes.

Response: We agree that health plans should be able to disclose protected health information to employers sponsoring health plans under certain circumstances. Section 164.504(f) explains the conditions under which protected health information may be disclosed to plan sponsors. We believe that this provision gives sponsors access to the information they need, but protects individual's information to the extent possible under our legislative authority.

Group Health Plan

For response to comments relating to ''group health plan,'' see the response to comments on ''health plan'' below and the response to comments on § 164.504.

Health Care

Comment: A number of commenters asked that we include disease management activities and other similar health improvement programs, such as preventive medicine, health education services and maintenance, health and case management, and risk assessment, in the definition of ''health care.'' Commenters maintained that the rule should avoid limiting technological advances and new health care trends intended to improve patient ''health care.''

Response: Review of these and other comments, and our fact-finding, indicate that there are multiple, different, understandings of the definition of these terms. Therefore, rather than create a blanket rule that includes such terms in or excludes such terms from the definition of ''health care,'' we define health care based on the underlying activities that constitute health care. The activities described by these commenters are considered ''health care'' under this rule to the extent that they meet this functional definition. Listing activities by label or title would create the risk that important activities would be left out and, given the lack of consensus on what these terms mean, could also create confusion.

Comment: Several commenters urged that the Department clarify that the activities necessary to procure and distribute eyes and eye tissue will not be hampered by the rule. Some of these commenters explicitly requested that we include ''eyes and eye tissue'' in the list of procurement biologicals as well as ''eye procurement'' in the definition of ''health care.'' In addition, it was argued that ''administration to patients'' be excluded in the absence of a clear definition. Also, commenters recommended that the definition include other activities associated with the transplantation of organs, such as processing, screening, and distribution.

Response: We delete from the definition of ''health care'' activities related to the procurement or banking of blood, sperm, organs, or any other tissue for administration to patients. We do so because persons who make such donations are not seeking to be treated, diagnosed, or assessed or otherwise seeking health care for themselves, but are seeking to contribute to the health care of others. In addition, the nature of

these activities entails a unique kind of information sharing and tracking necessary to safeguard the nation's organ and blood supply, and those seeking to donate are aware that this information sharing will occur. Consequently, such procurement or banking activities are not considered health care and the organizations that perform such activities are not considered health care providers for purposes of this rule.

With respect to disclosure of protected health information by covered entities to facilitate cadaveric organ and tissue donation, the final rule explicitly permits a covered entity to disclose protected health information without authorization, consent, or agreement to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating donation and transplantation. See § 164.512(h). We do not include blood or sperm banking in this provision because, for those activities, there is direct contact with the donor, and thus opportunity to obtain the individual's authorization.

Comment: A large number of commenters urged that the term ''assessment'' be included in the list of services in the definition, as ''assessment'' is used to determine the baseline health status of an individual. It was explained that assessments are conducted in the initial step of diagnosis and treatment of a patient. If assessment is not included in the list of services, they pointed out that the services provided by occupational health nurses and employee health information may not be covered.

Response: We agree and have added the term ''assessment'' to the definition to clarify that this activity is considered ''health care'' for the purposes of the rule.

Comment: One commenter asked that we revise the definition to explicitly exclude plasmapheresis from paragraph (3) of the definition. It was explained that plasmapheresis centers do not have direct access to health care recipients or their health information, and that the limited health information collected about plasma donors is not used to provide health care services as indicated by the definition of health care.

Response: We address the commenters' concerns by removing the provision related to procurement and banking of human products from the definition.

Health Care Clearinghouse

Comment: The largest set of comments relating to health care clearinghouses focused on our proposal to exempt health care clearinghouses from the patient notice and access rights provisions of the regulation. In our NPRM, we proposed to exempt health care clearinghouses from certain provisions of the regulation that deal with the covered entities' notice of information practices and consumers' rights to inspect, copy, and amend their records. The rationale for this exemption was based on our belief that health care clearinghouses engage primarily in business-to-business transactions and do not initiate or maintain direct relationships with individuals. We proposed this position with the caveat that the exemptions would be void for any health care clearinghouse that had direct contact with individuals in a capacity other than that of a business partner. In addition, we indicated that, in most instances, clearinghouses also would be considered business partners under this rule and would be bound by their contracts with covered plans and providers. They also would be subject to the notice of information practices developed by the plans and providers with whom they contract.

Commenters stated that, although health care clearinghouses do not have direct contact with individuals, they do have individually identifiable health information that may be subject to misuse or inappropriate disclosure. They expressed concern that we were proposing to exempt health care clearinghouses from all or many aspects of the regulation. These commenters suggested that we either delete the exemption or make it very narrow, specific and explicit in the final regulatory text.

Clearinghouse commenters, on the other hand, were in agreement with our proposal, including the exemption provision and the provision that the exemption is voided when the entity does have direct contact with individuals. They also stated that a health care clearinghouse that has a direct contact with individuals is no longer a health care clearinghouse as defined and should be subject to all requirements of the regulation.

Response: In the final rule, where a clearinghouse creates or receives protected health information as a business associate of another covered entity, we maintain the exemption for health care clearinghouses from certain provisions of the regulation dealing with the notice of information practices and patient's direct access rights to inspect, copy and amend records (§§ 164.524 and 164.526), on the grounds that a health care clearinghouse is engaged in business-to-business operations, and is not dealing directly with individuals. Moreover, as business associates of plans and providers, health care clearinghouses are bound by the notices of information practices of the covered entities with whom they contract.

Where a health care clearinghouse creates or receives protected health information other than as a business associate, however, it must comply with all the standards, requirements, and implementation specifications of the rule. We describe and delimit the exact nature of the exemption in the regulatory text. See § 164.500(b). We will monitor developments in this sector should the basic business-to-business relationship change.

Comment: A number of comments relate to the proposed definition of health care clearinghouse. Many commenters suggested that we expand the definition. They suggested that additional types of entities be included in the definition of health care clearinghouse, specifically medical transcription services, billing services, coding services, and ''intermediaries.'' One commenter suggested that the definition be expanded to add entities that receive standard transactions, process them and clean them up, and then send them on, without converting them to any standard format. Another commenter suggested that the health care clearinghouse definition be expanded to include entities that do not perform translation but may receive protected health information in a standard format and have access to that information. Another commenter stated that the list of covered entities should include any organization that receives or maintains individually identifiable health information. One organization recommended that we expand the health care clearinghouse definition to include the concept of a research data clearinghouse, which would collect individually identifiable health information from other covered entities to generate research data files for release as de-identified data or with appropriate confidentiality safeguards. One commenter stated that HHS had gone beyond Congressional intent by including billing services in the definition.

Response: We cannot expand the definition of ''health care clearinghouse'' to cover entities not covered by the definition of this term in the statute. In the final regulation, we

make a number of changes to address public comments relating to definition. We modify the definition of health care clearinghouse to conform to the definition published in the Transactions Rule (with the addition of a few words, as noted above). We clarify in the preamble that, while the term ''health care clearinghouse'' may have other meanings and connotations in other contexts, for purposes of this regulation an entity is considered a health care clearinghouse only to the extent that it actually meets the criteria in our definition. Entities performing other functions but not meeting the criteria for a health care clearinghouse are not clearinghouses, although they may be business associates. Billing services are included in the regulatory definition of ''health care clearinghouse,'' if they perform the specified clearinghouse functions. Although we have not added or deleted any entities from our original definition, we will monitor industry practices and may add other entities in the future as changes occur in the health system.

Comment: Several commenters suggested that we clarify that an entity acting solely as a conduit through which individually identifiable health information is transmitted or through which protected health information flows but is not stored is not a covered entity, e.g., a telephone company or Internet Service Provider. Other commenters indicated that once a transaction leaves a provider or plan electronically, it may flow through several entities before reaching a clearinghouse. They asked that the regulation protect the information in that interim stage, just as the security NPRM established a chain of trust arrangement for such a network. Others noted that these ''conduit'' entities are likely to be business partners of the provider, clearinghouse or plan, and we should clarify that they are subject to business partner obligations as in the proposed Security Rule.

Response: We clarify that entities acting as simple and routine communications conduits and carriers of information, such as telephone companies and Internet Service Providers, are not clearinghouses as defined in the rule unless they carry out the functions outlined in our definition. Similarly, we clarify that value added networks and switches are not health care clearinghouses unless they carry out the functions outlined in the definition, and clarify that such entities may be business associates if they meet the definition in the regulation.

Comment: Several commenters, including the large clearinghouses and their trade associations, suggested that we not treat health care clearinghouses as playing a dual role as covered entity and business partner in the final rule because such a dual role causes confusion as to which rules actually apply to clearinghouses. In their view, the definition of health care clearinghouse is sufficiently clear to stand alone and identify a health care clearinghouse as a covered entity, and allows health care clearinghouses to operate under one consistent set of rules.

Response: For reasons explained in § 164.504 of this preamble, we do not create an exception to the business associate requirements when the business associate is also a covered entity. We retain the concept that a health care clearinghouse may be a covered entity and a business associate of a covered entity under the regulation. As business associates, they would be bound by their contracts with covered plans and providers.

Health Care Provider

Comment: One commenter pointed out that the preamble referred to the obligations of providers and did not use the term, ''covered entity,'' and thus created ambiguity about the obligations of health care providers who may be employed by persons other than covered entities, e.g., pharmaceutical companies. It was suggested that a better reading of the statute and rule is that where neither the provider nor the company is a covered entity, the rule does not impose an obligation on either the provider-employee or the employer.

Response: We agree. We use the term ''covered entity'' whenever possible in the final rule, except for the instances where the final rule treats the entities differently, or where use of the term ''health care provider'' is necessary for purposes of illustrating an example.

Comment: Several commenters stated that the proposal's definition was broad, unclear, and/or confusing. Further, we received many comments requesting clarification as to whether specific entities or persons were ''health care providers'' for the purposes of our rule. One commenter questioned whether affiliated members of a health care group (even though separate legal entities) would be considered as one primary health care provider.

Response: We permit legally distinct covered entities that share common ownership or control to designate themselves together to be a single covered entity. Such organizations may promulgate a single shared notice of information practices and a consent form. For more detailed information, see the preamble discussion of § 164.504(d).

We understand the need for additional guidance on whether specific entities or persons are health care providers under the final rule. We provide guidance below and will provide additional guidance as the rule is implemented.

Comment: One commenter observed that sections 1171(3), 1861(s) and 1861(u) of the Act do not include pharmacists in the definition of health care provider or pharmacist services in the definition of ''medical or other health services,'' and questioned whether pharmacists were covered by the rule.

Response: The statutory definition of ''health care provider'' at section 1171(3) includes ''any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.'' Pharmacists' services are clearly within this statutory definition of ''health care.'' There is no basis for excluding pharmacists who meet these statutory criteria from this regulation.

Comment: Some commenters recommended that the scope of the definition be broadened or clarified to cover additional persons or organizations. Several commenters argued for expanding the reach of the health care provider definition to cover entities such as state and local public health agencies, maternity support services (provided by nutritionists, social workers, and public health nurses and the Special Supplemental Nutrition Program for Women, Infants and Children), and those companies that conduct cost-effectiveness reviews, risk management, and benchmarking studies. One commenter queried whether auxiliary providers such as child play therapists, and speech and language therapists are considered to be health care providers. Other commenters questioned whether ''alternative'' or ''complementary'' providers, such as naturopathic physicians and acupuncturists would be considered health care providers covered by the rule.

Response: As with other aspects of this rule, we do not define ''health care provider'' based on the title or label of the professional. The professional activities of these kinds of providers vary; a person is a ''health care provider'' if those activities are consistent with the rule's definition of ''health care provider.'' Thus, health care providers include persons, such as those noted by the commenters, to the extent that they meet the definition. We note that health care providers are only

subject to this rule if they conduct certain transactions. See the definition of ''covered entity.''

However companies that conduct cost-effectiveness reviews, risk management, and benchmarking studies are not health care providers for the purposes of this rule unless they perform other functions that meet the definition. These entities would be business associates if they perform such activities on behalf of a covered entity.

Comment: Another commenter recommended that the Secretary expand the definition of health care provider to cover health care providers who transmit or ''or receive'' any health care information in electronic form.

Response: We do not accept this suggestion. Section 1172(a)(3) states that providers that ''transmit'' health information in connection with one of the HIPAA transactions are covered, but does not use the term ''receive'' or a similar term.

Comment: Some comments related to online companies as health care providers and covered entities. One commenter argued that there was no reason ''why an Internet pharmacy should not also be covered'' by the rule as a health care provider. Another commenter stated that online health care service and content companies, including online medical record companies, should be covered by the definition of health care provider. Another commenter pointed out that the definitions of covered entities cover ''Internet providers who 'bill' or are 'paid' for health care services or supplies, but not those who finance those services in other ways, such as through sale of identifiable health information or advertising.'' It was pointed out that thousands of Internet sites use information provided by individuals who access the sites for marketing or other purposes.

Response: We agree that online companies are covered entities under the rule if they otherwise meet the definition of health care provider or health plan and satisfy the other requirements of the rule, i.e., providers must also transmit health information in electronic form in connection with a HIPAA transaction. We restate here the language in the preamble to the proposed rule that ''An individual or organization that bills and/or is paid for health care services or supplies in the normal course of business, such as * * * an ''online'' pharmacy accessible on the Internet, is also a health care provider for purposes of this statute'' (64 FR 59930).

Comment: We received many comments related to the reference to ''health clinic or licensed health care professional located at a school or business in the preamble's discussion of ''health care provider.'' It was stated that including ''licensed health care professionals located at a school or business'' highlights the need for these individuals to understand they have the authority to disclose information to the Social Security Administration (SSA) without authorization.

However, several commenters urged HHS to create an exception for or delete that reference in the preamble discussion to primary and secondary schools because of employer or business partner relationships. One federal agency suggested that the reference ''licensed health care professionals located at a [school]'' be deleted from the preamble because the definition of health care provider does not include a reference to schools. The commenter also suggested that the Secretary consider: adding language to the preamble to clarify that the rules do not apply to clinics or school health care providers that only maintain records that have been excepted from the definition of protected health information, adding an exception to the definition of covered entities for those schools, and limiting paperwork requirements for these schools. Another commenter argued for deleting references to schools because the proposed rule appeared to supersede or create ambiguity as to the Family Educational Rights and Privacy Act (FERPA), which gives parents the right to access ''education'' and health records of their unemancipated minor children. However, in contrast, one commenter supported the inclusion of health care professionals who provide services at schools or businesses.

Response: We realize that our discussion of schools in the NPRM may have been confusing. Therefore, we address these concerns and set forth our policy regarding protected health information in educational agencies and institutions in the ''Relationship to Other Federal Laws'' discussion of FERPA, above.

Comment: Many commenters urged that direct contact with the patient be necessary for an entity to be considered a health care provider. Commenters suggested that persons and organizations that are remote to the patient and have no direct contact should not be considered health care providers. Several commenters argued that the definition of health care provider covers a person that provides health care services or supplies only when the provider furnishes to or bills the patient directly. It was stated that the Secretary did not intend that manufacturers, such as pharmaceutical, biologics, and device manufacturers, health care suppliers, medical-surgical supply distributors, health care vendors that offer medical record documentation templates and that typically do not deal directly with the patient, be considered health care providers and thus covered entities. However, in contrast, one commenter argued that, as an in vitro diagnostics manufacturer, it should be covered as a health care provider.

Response: We disagree with the comments that urged that direct dealings with an individual be a prerequisite to meeting the definition of health care provider. Many providers included in the statutory definition of provider, such as clinical labs, do not have direct contact with patients. Further, the use and disclosure of protected health information by indirect treatment providers can have a significant effect on individuals' privacy. We acknowledge, however, that providers who treat patients only indirectly need not have the full array of responsibilities as direct treatment providers, and modify the NPRM to make this distinction with respect to several provisions (see, for example § 164.506 regarding consent). We also clarify that manufacturers and health care suppliers who are considered providers by Medicare are providers under this rule.

Comment: Some commenters suggested that blood centers and plasma donor centers that collect and distribute source plasma not be considered covered health care providers because the centers do not provide ''health care services'' and the blood donors are not ''patients'' seeking health care. Similarly, commenters expressed concern that organ procurement organizations might be considered health care providers.

Response: We agree and have deleted from the definition of ''health care'' the term ''procurement or banking of blood, sperm, organs, or any other tissue for administration to patients.'' See prior discussion under ''health care.''

Comment: Several commenters proposed to restrict coverage to only those providers who furnished and were paid for services and supplies. It was argued that a salaried employee of a covered entity, such as a hospital-based provider, should not be covered by the rule because that provider would be subject both directly to the rule as a covered entity and indirectly as an employee of a covered entity.

Response: The ''dual'' direct and indirect situation described in these comments can arise only when a health

care provider conducts standard HIPAA transactions both for itself and for its employer. For example, when the services of a provider such as a hospital-based physician are billed through a standard HIPAA transaction conducted for the employer, in this example the hospital, the physician does not become a covered provider. Only when the provider uses a standard transaction on its own behalf does he or she become a covered health care provider. Thus, the result is typically as suggested by this commenter. When a hospital-based provider is not paid directly, that is, when the standard HIPAA transaction is not on its behalf, it will not become a covered provider.

Comment: Other commenters argued that an employer who provides health care services to its employees for whom it neither bills the employee nor pays for the health care should not be considered health care providers covered by the proposed rule.

Response: We clarify that the employer may be a health care provider under the rule, and may be covered by the rule if it conducts standard transactions. The provisions of § 164.504 may also apply.

Comment: Some commenters were confused about the preamble statement: ''in order to implement the principles in the Secretary's Recommendations, we must impose any protections on the health care providers that use and disclose the information, rather than on the researcher seeking the information,'' with respect to the rule's policy that a researcher who provides care to subjects in a trial will be considered a health care provider. Some commenters were also unclear about whether the individual researcher providing health care to subjects in a trial would be considered a health care provider or whether the researcher's home institution would be considered a health care provider and thus subject to the rule.

Response: We clarify that, in general, a researcher is also a health care provider if the researcher provides health care to subjects in a clinical research study and otherwise meets the definition of ''health care provider'' under the rule. However, a health care provider is only a covered entity and subject to the rule if that provider conducts standard transactions. With respect to the above preamble statement, we meant that our jurisdiction under the statute is limited to covered entities. Therefore, we cannot apply any restrictions or requirements on a researcher in that person's role as a researcher. However, if a researcher is also a health care provider that conducts standard transactions, that researcher/provider is subject to the rule with regard to its provider activities.

As to applicability to a researcher/provider versus the researcher's home institution, we provide the following guidance. The rule applies to the researcher as a covered entity if the researcher is a health care provider who conducts standard transactions for services on his or her own behalf, regardless of whether he or she is part of a larger organization. However, if the services and transactions are conducted on behalf of the home institution, then the home institution is the covered entity for purposes of the rule and the researcher/provider is a workforce member, not a covered entity.

Comment: One commenter expressed confusion about those instances when a health care provider was a covered entity one day, and one who ''works under a contract'' for a manufacturer the next day.

Response: If persons are covered under the rule in one role, they are not necessarily covered entities when they participate in other activities in another role. For example, that person could be a covered health care provider in a hospital one day but the next day read research records for a different employer. In its role as researcher, the person is not covered, and protections do not apply to those research records.

Comment: One commenter suggested that the Secretary modify proposed § 160.102, to add the following clause at the end (after (c)) (regarding health care provider), ''With respect to any entity whose *primary* business is not that of a health plan or health care provider licensed under the applicable laws of any state, the standards, requirements, and implementation specifications of this subchapter shall apply solely to the component of the entity that engages in the transactions specified in [§] 160.103.'' (Emphasis added.) Another commenter also suggested that the definition of ''covered entity'' be revised to mean entities that are ''primarily or exclusively engaged in health care-related activities as a health plan, health care provider, or health care clearinghouse.''

Response: The Secretary rejects these suggestions because they will impermissibly limit the entities covered by the rule. An entity that is a health plan, health care provider, or health care clearinghouse meets the statutory definition of covered entity regardless of how much time is devoted to carrying out health care-related functions, or regardless of what percentage of their total business applies to health care-related functions.

Comment: Several commenters sought to distinguish a health care provider from a business partner as proposed in the NPRM. For example, a number of commenters argued that disease managers that provide services ''on behalf of'' health plans and health care providers, and case managers (a variation of a disease management service) are business partners and not ''health care providers.'' Another commenter argued that a disease manager should be recognized (presumably as a covered entity) because of its involvement from the physician-patient level through complex interactions with health care providers.

Response: To the extent that a disease or case manager provides services on behalf of or to a covered entity as described in the rule's definition of business associate, the disease or case manager is a business associate for purposes of this rule. However, if services provided by the disease or case manager meet the definition of treatment and the person otherwise meets the definition of ''health care provider,'' such a person is a health care provider for purposes of this rule.

Comment: One commenter argued that pharmacy employees who assist pharmacists, such as technicians and cashiers, are not business partners.

Response: We agree. Employees of a pharmacy that is a covered entity are workforce members of that covered entity for purposes of this rule.

Comment: A number of commenters requested that we clarify the definition of health care provider (''* * * who furnishes, bills, or is paid for health care services or supplies in the normal course of business'') by defining the various terms ''furnish'', ''supply'', and ''in the normal course of business.'' For instance, it was stated that this would help employers recognize when services such as an employee assistance program constituted health care covered by the rule.

Response: Although we understand the concern expressed by the commenters, we decline to follow their suggestion to define terms at this level of specificity. These terms are in common use today, and an attempt at specific definition would risk the inadvertent creations of conflict with industry practices. There is a significant variation in the way employers structure their employee assistance programs (EAPs) and the type of services that they provide. If the EAP provides direct treatment to individuals, it may be a health care provider.

Health Information

The response to comments on health information is included in the response to comments on individually identifiable health information, in the preamble discussion of § 164.501.

Health Plan

Comment: One commenter suggested that to eliminate any ambiguity, the Secretary should clarify that the catch-all category under the definition of health plan includes ''24-hour coverage plans'' (whether insured or self-insured) that integrate traditional employee health benefits coverage and workers' compensation coverage for the treatment of on-the-job injuries and illnesses under one program. It was stated that this clarification was essential if the Secretary persisted in excluding workers' compensation from the final rule.

Response: We understand concerns that such plans may use and disclose individually identifiable health information. We therefore clarify that to the extent that 24-hour coverage plans have a health care component that meets the definition of ''health plan'' in the final rule, such components must abide by the provisions of the final rule. In the final rule, we have added a new provision to § 164.512 that permits covered entities to disclose information under workers' compensation and similar laws. A health plan that is a 24-hour plan is permitted to make disclosures as necessary to comply with such laws.

Comment: A number of commenters urged that certain types of insurance entities, such as workers' compensation and automobile insurance carriers, property and casualty insurance health plans, and certain forms of limited benefits coverage, be included in the definition of ''health plan.'' It was argued that consumers deserve the same protection with respect to their health information, regardless of the entity using it, and that it would be inequitable to subject health insurance carriers to more stringent standards than other types of insurers that use individually identifiable health information.

Response: The Congress did not include these programs in the definition of a ''health plan'' under section 1171 of the Act. Further, HIPAA's legislative history shows that the House Report's (H. Rep. 104–496) definition of ''health plan'' originally included certain benefit programs, such as workers' compensation and liability insurance, but was later amended to clarify the definition and remove these programs. Thus, since the statutory definition of a health plan both on its face and through legislative history evidence Congress' intention to exclude such programs, we do not have the authority to require that these programs comply with the standards. We have added explicit language to the final rule which excludes the excepted benefit programs, as defined in section 2971(c)(1) of the PHS Act, 42 U.S.C. 300gg-91(c)(1).

Comment: Some commenters urged HHS to include entities such as stop loss insurers and reinsurers in the definition of ''health plan.'' It was observed that such entities have come to play important roles in managed care delivery systems. They asserted that increasingly, capitated health plans and providers contract with their reinsurers and stop loss carriers to medically manage their high cost outlier cases such as organ and bone marrow transplants, and therefore should be specifically cited as subject to the regulations.

Response: Stop-loss and reinsurers do not meet the statutory definition of health plan. They do not provide or pay for the costs of medical care, as described in the statute, but rather insure health plans and providers against unexpected losses. Therefore, we cannot include them as health plans in the regulation.

Comment: A commenter asserted that there is a significant discrepancy between the effect of the definition of ''group health plan'' as proposed in § 160.103, and the anticipated impact in the cost estimates of the proposed rule at 64 FR 60014. Paragraph (1) of the proposed definition of ''health plan'' defined a ''group health plan'' as an ERISA-defined employee welfare benefit plan that provides medical care and that: ''(i) Has 50 or more participants, *or* (ii) Is administered by an entity other than the employer that established and maintains the plan[.]'' (emphasis added) According to this commenter, under this definition, the only insured or self-insured ERISA plans that would not be regulated ''health plans'' would be those that have less than 50 participants and are self administered.

The commenter presumed that the we had intended to exclude from the definition of ''health plan'' (and from coverage under the proposed rule) all ERISA plans that are small (less than 50 participants) *or* are administered by a third party, whether large or small, based on the statement at 64 FR 60014, note 18. That footnote stated that the Department had ''not included the 3.9 million 'other' employer-health plans listed in HCFA's administrative simplification regulations because these plans are administered by a third party. The proposed regulation will not regulate the employer plans but will regulate the third party administrators of the plan.'' The commenter urged us not to repeat the statutory definition, and to adopt the policy implied in the footnote.

Response: We agree with the commenter's observation that footnote 18 (64 FR 60014) was inconsistent with the proposed definition. We erred in drafting that note. The definition of ''group health plan'' is adopted from the statutory definition at section 1171(5)(A), and excludes from the rule as ''health plans'' only the few insured or self-insured ERISA plans that have less than 50 participants *and* are self administered. We reject the commenter's proposed change to the definition as inconsistent with the statute.

Comment: A number of insurance companies asked that long term care insurance policies be excluded from the definition of ''health plan.'' It was argued that such policies do not provide sufficiently comprehensive coverage of the cost of medical care, and are limited benefit plans that provide or pay for the cost of custodial and other related services in connection with a long term, chronic illness or disability.

These commenters asserted that HIPAA recognizes this nature of long term care insurance, observing that, with respect to HIPAA's portability requirements, Congress enacted a series of exclusions for certain defined types of health plan arrangements that do not typically provide comprehensive coverage. They maintained that Congress recognized that long term care insurance is excluded, so long as it is not a part of a group health plan. Where a long term care policy is offered separately from a group health plan it is considered an excepted benefit and is not subject to the portability and guarantee issue requirements of HIPAA. Although this exception does not appear in the Administrative Simplification provisions of HIPAA, it was asserted that it is guidance with respect to the treatment of long term care insurance as a limited benefit coverage and not as coverage that is so ''sufficiently comprehensive'' that it is to be treated in the same manner as a typical, comprehensive major medical health plan arrangement.

Another commenter offered a different perspective observing that there are some long-term care policies—that do not pay for medical care and therefore are not ''health plans.'' It was noted that most long-term care policies are reimbursement policies—that is,

they reimburse the policyholder for the actual expenses that the insured incurs for long-term care services. To the extent that these constitute ''medical care,'' this commenter presumed that these policies would be considered ''health plans.'' Other long-term care policies, they pointed out, simply pay a fixed dollar amount when the insured becomes chronically ill, without regard to the actual cost of any long-term care services received, and thus are similar to fixed indemnity critical illness policies. The commenter suggested that while there was an important distinction between indemnity based long-term care policies and expenses based long-term care policies, it may be wise to exclude all long-term care policies from the scope of the rule to achieve consistency with HIPAA.

Response: We disagree. The statutory language regarding long-term care policies in the portability title of HIPAA is different from the statutory language regarding long-term care policies in the Administrative Simplification title of HIPAA. Section 1171(5)(G) of the Act means that issuers of long-term care policies are considered health plans for purposes of administrative simplification. We also interpret the statute as authorizing the Secretary to exclude nursing home fixed-indemnity policies, not all long-term care policies, from the definition of ''health plan,'' if she determines that these policies do not provide ''sufficiently comprehensive coverage of a benefit'' to be treated as a health plan (see section 1171 of the Act). We interpret the term ''comprehensive'' to refer to the breadth or scope of coverage of a policy. ''Comprehensive'' policies are those that cover a range of possible service options. Since nursing home fixed indemnity policies are, by their own terms, limited to payments made solely for nursing facility care, we have determined that they should not be included as health plans for the purposes of the HIPAA regulations. The Secretary, therefore, explicitly excluded nursing home fixed-indemnity policies from the definition of ''health plan'' in the Transactions Rule, and this exclusion is thus reflected in this final rule. Issuers of other long-term care policies are considered to be health plans under this rule and the Transactions Rule.

Comment: One commenter was concerned about the potential impact of the proposed regulations on ''unfunded health plans,'' which the commenter described as programs used by smaller companies to provide their associates with special employee discounts or other membership incentives so that they can obtain health care, including prescription drugs, at reduced prices. The commenter asserted that if these discount and membership incentive programs were covered by the regulation, many smaller employers might discontinue offering them to their employees, rather than deal with the administrative burdens and costs of complying with the rule.

Response: Only those special employee discounts or membership incentives that are ''employee welfare benefit plans'' as defined in section 3(1) of the Employee Retirement Income Security Act of 1974, 29 U.S.C. 1002(1), and provide ''medical care'' (as defined in section 2791(a)(2) of the Public Health Service Act, 42 U.S.C. 300gg-91(a)(2)), are health plans for the purposes of this rule. Discount or membership incentive programs that are not group health plans are not covered by the rule.

Comment: Several commenters agreed with the proposal to exclude ''excepted benefits'' such as disability income insurance policies, fixed indemnity critical illness policies, and per diem long-term care policies from the definition of ''health plan,'' but were concerned that the language of the proposed rule did not fully reflect this intent. They asserted that clarification was necessary in order to avoid confusion and costs to both consumers and insurers.

One commenter stated that, while HHS did not intend for the rule to apply to every type of insurance coverage that paid for medical care, the language of the proposed rule did not bear this out. The problem, it was asserted, is that under the proposed rule any insurance policy that pays for ''medical care'' would technically be a ''health plan.'' It was argued that despite the statements in the narrative, there are no provisions that would exempt any of the ''excepted benefits'' from the definition of ''health care.'' It was stated that:

> Although (with the exception of long-term care insurance), the proposed rule does not include the 'excepted benefits' in its list of sixteen examples of a health plan (proposed 45 CFR 160.104), it does not explicitly exclude them either. Because these types of policies in some instances pay benefits that could be construed as payments for medical care, we are concerned by the fact that they are not explicitly excluded from the definition of 'health plan' or the requirements of the proposed rule.''

Several commenters proposed that HHS adopt the same list of ''excepted benefits'' contained in 29 U.S.C. 1191b, suggesting that they could be adopted either as exceptions to the definition of ''health plan'' or as exceptions to the requirements imposed on ''health plans.'' They asserted that this would promote consistency in the federal regulatory structure for health plans.

It was suggested that HHS clarify whether the definition of health plan, particularly the ''group health plan'' and ''health insurance issuer'' components, includes a disability plan or disability insurer. It was noted that a disability plan or disability insurer may cover only income lost from disability and, as mentioned above, some rehabilitation services, or a combination of lost income, rehabilitation services and medical care. The commenter suggested that in addressing this coverage issue, it may be useful to refer to the definitions of group health plan, health insurance issuer and medical care set forth in Part I of HIPAA, which the statutory provisions of the Administrative Simplification subtitle expressly reference. See 42 U.S.C. 1320d(5)(A) and (B).

Response: We agree that the NPRM may have been ambiguous regarding the types of plans the rule covers. To remedy this confusion, we have added language that specifically excludes from the definition any policy, plan, or program providing or paying the cost of the excepted benefits, as defined in section 2971(c)(1) of the PHS Act, 42 U.S.C. 300gg–91(c)(1). As defined in the statute, this includes but is not limited to benefits under one or more (or any combination thereof) of the following: coverage only for accident, or disability income insurance, or any combination thereof; liability insurance, including general liability insurance and automobile liability insurance; and workers' compensation or similar insurance.

However, the other excepted benefits as defined in section 2971(c)(2) of the PHS Act, 42 U.S.C. 300gg–91(c)(2), such as limited scope dental or vision benefits, not explicitly excepted from the regulation could be considered ''health plans'' under paragraph (1)(xvii) of the definition of ''health plan'' in the final rule if and to the extent that they meet the criteria for the definition of ''health plan.'' Such plans, unlike the programs and plans listed at section 2971(c)(1), directly and exclusively provide health insurance, even if limited in scope.

Comment: One commenter recommended that the Secretary clarify that ''health plan'' does not include property and casualty benefit providers. The commenter stated that the clarifying language is needed given the ''catchall'' category of entities defined as ''any other individual plan or group health plan, or combination thereof, that

provides or pays for the cost of medical care,'' and asserted that absent clarification there could be serious confusion as to whether property and casualty benefit providers are ''health plans'' under the rule.

Response: We agree and as described above have added language to the final rule to clarify that the ''excepted benefits'' as defined under 42 U.S.C. 300gg–91(c)(1), which includes liability programs such as property and casualty benefit providers, are not health plans for the purposes of this rule.

Comment: Some commenters recommended that the Secretary replace the term ''medical care'' with ''health care.'' It was observed that ''health care'' was defined in the proposal, and that this definition was used to define what a health care provider does. However, they observed that the definition of ''health plan'' refers to the provision of or payment for ''medical care,'' which is not defined. Another commenter recommended that HHS add the parenthetical phrase ''as such term is defined in section 2791 of the Public Health Service Act'' after the phrase ''medical care.''

Response: We disagree with the first recommendation. We understand that the term ''medical care'' can be easily confused with the term ''health care.'' However, the two terms are not synonymous. The term ''medical care'' is a statutorily defined term and its use is critical in making a determination as to whether a health plan is considered a ''health plan'' for purposes of administrative simplification. In addition, since the term ''medical care'' is used in the regulation only in the context of the definition of ''health plan'' and we believe that its inclusion in the regulatory text may cause confusion, we did not add a definition of ''medical care'' in the final rule. However, consistent with the second recommendation above, the statutory cite for ''medical care'' was added to the definition of ''health plan'' in the Transactions Rule, and thus is reflected in this final rule.

Comment: A number of commenters urged that the Secretary define more narrowly what characteristics would make a government program that pays for specific health care services a ''health plan.'' Commenters argued that there are many ''payment'' programs that should not be included, as discussed below, and that if no distinctions were made, ''health plan'' would mean the same as ''purchaser'' or even ''payor.''

Commenters asserted that there are a number of state programs that pay for ''health care'' (as defined in the rule) but that are not health plans. They said that examples include the WIC program (Special Supplemental Nutrition Program for Women, Infants, and Children) which pays for nutritional assessment and counseling, among other services; the AIDS Client Services Program (including AIDS prescription drug payment) under the federal Ryan White Care Act and state law; the distribution of federal family planning funds under Title X of the Public Health Services Act; and the breast and cervical health program which pays for cancer screening in targeted populations. Commenters argued that these are not insurance plans and do not fall within the ''health plan'' definition's list of examples, all of which are either insurance or broad-scope programs of care under a contract or statutory entitlement. However, paragraph (16) in that list opens the door to broader interpretation through the catchall phrase, ''any other individual or group plan that provides or pays for the cost of medical care.'' Commenters assert that clarification is needed.

A few commenters stated that other state agencies often work in partnership with the state Medicaid program to implement certain Medicaid benefits, such as maternity support services and prenatal genetics screening. They concluded that while this probably makes parts of the agency the ''business partner'' of a covered entity, they were uncertain whether it also makes the same agency parts a ''health plan'' as well.

Response: We agree with the commenters that clarification is needed as to the rule's application to government programs that pay for health care services. Accordingly, in the final rule we have excepted from the definition of ''health plan'' a government funded program which does not have as its principal purpose the provision of, or payment for, the cost of health care or which has as its principal purpose the provision, either directly or by grant, of health care. For example, the principal purpose of the WIC program is not to provide or pay for the cost of health care, and thus, the WIC program is not a health plan for purposes of this rule. The program of health care services for individuals detained by the INS provides health care directly, and so is not a health plan. Similarly, the family planning program authorized by Title X of the Public Health Service Act pays for care exclusively through grants, and so is not a health plan under this rule. These programs (the grantees under the Title X program) may be or include health care providers and may be covered entities if they conduct standard transactions.

We further clarify that, where a public program meets the definition of ''health plan,'' the government agency that administers the program is the covered entity. Where two agencies administer a program jointly, they are both a health plan. For example, both the Health Care Financing Administration and the insurers that offers a Medicare+Choice plan are ''health plans'' with respect to Medicare beneficiaries. An agency that does not administer a program but which provides services for such a program is not a covered entity by virtue of providing such services. Whether an agency providing services is a business associate of the covered entity depends on whether its functions for the covered entity meet the definition of business associate in § 164.501 and, in the example described by this comment, in particular on whether the arrangement falls into the exception in § 164.504(e)(1)(ii)(C) for government agencies that collect eligibility or enrollment information for covered government programs.

Comment: Some commenters expressed support for retaining the category in paragraph (16) of the proposal's definition: ''Any other individual or group health plan, or combination thereof, that provides or pays for the cost of medical care.'' Others asked that the Secretary clarify this category. One commenter urged that the final rule clearly define which plans would meet the criteria for this category.

Response: As described in the proposed rule, this category implements the language at the beginning of the statutory definition of the term ''health plan'': ''The term 'health plan' means an individual or group plan that provides, or pays the cost of, medical care * * * Such term includes the following, and any combination thereof * * *'' This statutory language is general, not specific, and as such, we are leaving it general in the final rule. However, as described above, we add explicit language which excludes certain ''excepted benefits'' from the definition of ''health plan'' in an effort to clarify which plans are not health plans for the purposes of this rule. Therefore, to the extent that a certain benefits plan or program otherwise meets the definition of ''health plan'' and is not explicitly excepted, that program or plan is considered a ''health plan'' under paragraph (1)(xvii) of the final rule.

Comment: A commenter explained that HIPAA defines a group health plan by expressly cross-referencing the statutory sections in the PHS Act and the Employee Retirement Income

Security Act of 1974 (ERISA), 29 U.S.C. 1001, *et seq.*, which define the terms ''group health plan,'' ''employee welfare benefit plan'' and ''participant.'' See 29 U.S.C. 1002(l) (definition of ''employee welfare benefit plan,'' which is the core of the definition of group health plan under both ERISA and the PHS Act); 29 U.S.C. 100217) (definition of participant); 29 U.S.C. 1193(a) (definition of ''group health plan,'' which is identical to that in section 2791(a) of the PHS Act).

It was pointed out that the preamble and the text of the proposed rule both limit the definition of all three terms to their current definitions. The commenter reasoned that since the ERISA definitions may change over time through statutory amendment, Department of Labor regulations or judicial interpretation, it would not be clear what point in time is to be considered current. Therefore, they suggested deleting references to ''current'' or ''currently'' in the preamble and in the regulation with respect to these three ERISA definitions.

In addition, the commenter stated that as the preamble to the NPRM correctly reflected, HIPAA expressly cross-references ERISA's definition of ''participant'' in section 3(7) of ERISA, 29 U.S.C. 1002(7). 42 U.S.C. 1320d(5)(A). The text of the privacy regulation, however, omits this cross-reference. It was suggested that the reference to section 3(7) of ERISA, defining ''participant,'' be included in the regulation.

Finally, HIPAA incorporates the definition of a group health plan as set forth in section 2791(a) of the PHS Act, 42 U.S.C. 300gg–91(a)(l). That definition refers to the provision of medical care ''directly or through insurance, reimbursement, or otherwise.'' The word ''reimbursement'' is omitted in both the preamble and the text of the regulation; the commenter suggested restoring it to both.

Response: We agree. These changes were made to the definition of ''health plan'' as promulgated in the Transactions Rule, and are reflected in this final rule.

Small Health Plan

Comment: One commenter recommended that we delete the reference to $5 million in the definition and instead define a ''small health plan'' as a health plan with fewer than 50 participants. It was stated that using a dollar limitation to define a ''small health plan'' is not meaningful for self-insured plans and some other types of health plan coverage arrangements. A commenter pointed out that the general definition of a health plan refers to ''50 or more participants,'' and that using a dollar factor to define a ''small health plan'' would be inconsistent with this definition.

Response: We disagree. The Small Business Administration (SBA) promulgates size standards that indicate the maximum number of employees or annual receipts allowed for a concern (13 CFR 121.105) and its affiliates to be considered ''small.'' The size standards themselves are expressed either in number of employees or annual receipts (13 CFR 121.201). The size standards for compliance with programs of other agencies are those for SBA programs which are most comparable to the programs of such other agencies, unless otherwise agreed by the agency and the SBA (13 CFR 121.902). With respect to the insurance industry, the SBA has specified that annual receipts of $5 million is the maximum allowed for a concern and its affiliates to be considered small (13 CFR 121.201). Consequently, we retain the proposal's definition in the final rule to be consistent with SBA requirements.

We understand there may be some confusion as to the meaning of ''annual receipts'' when applied to a health plan. For our purposes, therefore, we consider ''pure premiums'' to be equivalent to ''annual receipts.''

Workforce

Comment: Some commenters requested that we exclude ''volunteers'' from the definition of workforce. They stated that volunteers are important contributors within many covered entities, and in particular hospitals. They argued that it was unfair to ask that these people donate their time and at the same time subject them to the penalties placed upon the paid employees by these regulations, and that it would discourage people from volunteering in the health care setting.

Response: We disagree. We believe that differentiating those persons under the direct control of a covered entity who are paid from those who are not is irrelevant for the purposes of protecting the privacy of health information, and for a covered entity's management of its workforce. In either case, the person is working for the covered entity. With regard to implications for the individual, persons in a covered entity's workforce are not held personally liable for violating the standards or requirements of the final rule. Rather, the Secretary has the authority to impose civil monetary penalties and in some cases criminal penalties for such violations on only the covered entity.

Comment: One commenter asked that the rule clarify that employees administering a group health or other employee welfare benefit plan on their employers' behalf are considered part of the covered entity's workforce.

Response: As long as the employees have been identified by the group health plan in plan documents as performing functions related to the group health plan (consistent with the requirements of § 164.504(f)), those employees may have access to protected health information. However, they are not permitted to use or disclose protected health information for employment-related purposes or in connection with any other employee benefit plan or employee benefit of the plan sponsor.

Part 160—Subpart B—Preemption of State Law

We summarize and respond below to comments received in the Transactions rulemaking on the issue of preemption, as well as those received on this topic in the Privacy rulemaking. Because no process was proposed in the Transactions rulemaking for granting exceptions under section 1178(a)(2)(A), a process for making exception determinations was not adopted in the Transactions Rule. Instead, since a process for making exception determinations was proposed in the Privacy rulemaking, we decided that the comments received in the Transactions rulemaking should be considered and addressed in conjunction with the comments received on the process proposed in the Privacy rulemaking. See 65 FR 50318 for a fuller discussion. Accordingly, we discuss the preemption comments received in the Transactions rulemaking where relevant below.

Comment: The majority of comments on preemption addressed the subject in general terms. Numerous comments, particularly from plans and providers, argued that the proposed preemption provisions were burdensome, ineffective, or insufficient, and that complete federal preemption of the ''patchwork'' of state privacy laws is needed. They also argued that the proposed preemption provisions are likely to invite litigation. Various practical arguments in support of this position were made. Some of these comments recognized that the Secretary's authority under section 1178 of the Act is limited and acknowledged that the Secretary's proposals were within her statutory authority. One commenter suggested that the exception determination process would result in a very costly and laborious and sometimes inconsistent analysis of the occasions in which state law would

survive federal preemption, and thus suggested the final privacy regulations preempt state law with only limited exceptions, such as reporting child abuse. Many other comments, however, recommended changing the proposed preemption provisions to preempt state privacy laws on as blanket a basis as possible.

One comment argued that the assumption that more stringent privacy laws are better is not necessarily true, citing a 1999 GAO report finding evidence that the stringent state confidentiality laws of Minnesota halted the collection of comparative information on health care quality.

Several comments in this vein were also received in the Transactions rulemaking. The majority of these comments took the position that exceptions to the federal standards should either be prohibited or discouraged. It was argued that granting exceptions to the standards, particularly the transactions standards, would be inconsistent with the statute's objective of promoting administrative simplification through the use of uniform transactions.

Many other commenters, however, endorsed the ''federal floor'' approach of the proposed rules. (These comments were made in the context of the proposed privacy regulations.) These comments argued that this approach was preferable because it would not impair the effectiveness of state privacy laws that are more protective of privacy, while raising the protection afforded medical information in states that do not enact laws that are as protective as the rules below. Some comments argued, however, that the rules should give even more deference to state law, questioning in particular the definitions and the proposed addition to the ''other purposes'' criterion for exception determinations in this regard.

Response: With respect to the exception process provided for by section 1178(a)(2)(A), the contention that the HIPAA standards should uniformly control is an argument that should be addressed to the Congress, not this agency. Section 1178 of the Act expressly gives the Secretary authority to grant exceptions to the general rule that the HIPAA standards preempt contrary state law in the circumstances she determines come within the provisions at section 1178(a)(2)(A). We agree that the underlying statutory goal of standardizing financial and administrative health care transactions dictates that exceptions should be granted only on narrow grounds. Nonetheless, Congress clearly intended to accommodate some state laws in these areas, and the Department is not free to disregard this Congressional choice. As is more fully explained below, we have interpreted the statutory criteria for exceptions under section 1178(a)(2)(A) to balance the need for relative uniformity with respect to the HIPAA standards with state needs to set certain policies in the statutorily defined areas.

The situation is different with respect to state laws relating to the privacy of protected health information. Many of the comments arguing for uniform standards were particularly concerned with discrepancies between the federal privacy standards and various state privacy requirements. Unlike the situation with respect to the transactions standards, where states have generally not entered the field, all states regulate the privacy of some medical information to a greater or lesser extent. Thus, we understand the private sector's concern at having to reconcile differing state and federal privacy requirements.

This is, however, likewise an area where the policy choice has been made by Congress. Under section 1178(a)(2)(B) of the Act and section 264(c)(2) of HIPAA, provisions of state privacy laws that are contrary to and more stringent than the corresponding federal standard, requirement, or implementation specification are not preempted. The effect of these provisions is to let the law that is most protective of privacy control (the ''federal floor'' approach referred to by many commenters), and this policy choice is one with which we agree. Thus, the statute makes it impossible for the Secretary to accommodate the requests to establish uniformly controlling federal privacy standards, even if doing so were viewed as desirable.

Comment: Numerous comments stated support for the proposal at proposed Subpart B to issue advisory opinions with respect to the preemption of state laws relating to the privacy of individually identifiable health information. A number of these comments appeared to assume that the Secretary's advisory opinions would be dispositive of the issue of whether or not a state law was preempted. Many of these commenters suggested what they saw as improvements to the proposed process, but supported the proposal to have the Department undertake this function.

Response: Despite the general support for the advisory opinion proposal, we decided not to provide specifically for the issuance of such opinions. The following considerations led to this decision. First, the assumption by commenters that an advisory opinion would establish what law applied in a given situation and thereby simplify the task of ascertaining what legal requirements apply to a covered entity or entities is incorrect. Any such opinion would be advisory only. Although an advisory opinion issued by the Department would indicate to covered entities how the Department would resolve the legal conflict in question and would apply the law in determining compliance, it would not bind the courts. While we assume that most courts would give such opinions deference, the outcome could not be guaranteed.

Second, the thousands of questions raised in the public comment about the interpretation, implications, and consequences of all of the proposed regulatory provisions have led us to conclude that significant advice and technical assistance about all of the regulatory requirements will have to be provided on an ongoing basis. We recognize that the preemption concerns that would have been addressed by the proposed advisory opinions were likely to be substantial. However, there is no reason to assume that they will be the most substantial or urgent of the questions that will most likely need to be addressed. It is our intent to provide as much technical advice and assistance to the regulated community as we can with the resources available. Our concern is that setting up an advisory opinion process for just one of the many types of issues that will have to be addressed will lead to a non-optimal allocation of those resources. Upon careful consideration, therefore, we have decided that we will be better able to prioritize our workload and be better able to be responsive to the most urgent and substantial questions raised to the Department, if we do not provide for a formal advisory opinion process on preemption as proposed.

Comment: A few commenters argued that the Privacy Rule should preempt state laws that would impose more stringent privacy requirements for the conduct of clinical trials. One commenter asserted that the existing federal regulations and guidelines for patient informed consent, together with the proposed rule, would adequately protect patient privacy.

Response: The Department does not have the statutory authority under HIPAA to preempt state laws that would impose more stringent privacy requirements on covered entities. HIPAA provides that the rule promulgated by the Secretary may not preempt state laws that are in conflict

with the regulatory requirements and that provide greater privacy protections.

Section 160.201—Applicability

Comment: Several commenters indicated that the guidance provided by the definitions at proposed § 160.202 would be of substantial benefit both to regulated entities and to the public. However, these commenters argued that the applicability of such definitions would be too limited as drafted, since proposed § 160.201 provided that the definitions applied only to ''determinations and advisory opinions issued by the Secretary pursuant to 42 U.S.C. 1320d–7.'' The commenters stated that it would be far more helpful to make the definitions in proposed § 160.202 more broadly applicable, to provide general guidance on the issue of preemption.

Response: We agree with the comments on this issue, and have revised the applicability provision of subpart B below accordingly. Section 160.201 below sets out that Subpart B implements section 1178. This means, in our view, that the definitions of the statutory terms at § 160.202 are legislative rules that apply when those statutory terms are employed, whether by HHS, covered entities, or the courts.

Section 160.202—Definitions

Contrary

Comment: Some commenters asserted that term ''contrary'' as defined at § 160.202 was overly broad and that its application would be time-consuming and confusing for states. These commenters argued that, under the proposed definition, a state would be required to examine all of its laws relating to health information privacy in order to determine whether or not its law were contrary to the requirements proposed. It was also suggested that the definition contain examples of how it would work in practical terms.

A few commenters, however, argued that the definition of ''contrary'' as proposed was too narrow. One commenter argued that the Secretary erred in her assessment of the case law analyzing what is known as ''conflict preemption'' and which is set forth in shorthand in the tests set out at § 160.202.

Response: We believe that the definition proposed represents a policy that is as clear as is feasible and which can be applied nationally and uniformly. As was noted in the preamble to the proposed rules (at 64 FR 59997), the tests in the proposed definition of ''contrary'' are adopted from the jurisprudence of ''conflict preemption.'' Since preemption is a judicially developed doctrine, it is reasonable to interpret this term as indicating that the statutory analysis should tie in to the analytical formulations employed by the courts. Also, while the court-developed tests may not be as clear as commenters would like, they represent a long-term, thoughtful consideration of the problem of defining when a state/federal conflict exists. They will also, we assume, generally be employed by the courts when conflict issues arise under the rules below. We thus see no practical alternative to the proposed definition and have retained it unchanged. With respect to various suggestions for shorthand versions of the proposed tests, such as the arguably broader term ''inconsistent with,'' we see no operational advantages to such terms.

Comment: One comment asked that the Department clarify that if state law is not preempted, then the federal law would not also apply.

Response: This comment raises two issues, both of which deserve discussion. First, a state law may not be preempted because there is no conflict with the analogous federal requirement; in such a situation, both laws can, and must, be complied with. We thus do not accept this suggestion, to the extent that it suggests that the federal law would give way in this situation. Second, a state law may also not be preempted because it comes within section 1178(a)(2)(B), section 1178(b), or section 1178(c); in this situation, a contrary federal law would give way.

Comment: One comment urged the Department to take the position that where state law exists and no analogous federal requirement exists, the state requirement would not be ''contrary to'' the federal requirement and would therefore not trigger preemption.

Response: We agree with this comment.

Comment: One commenter criticized the definition as unhelpful in the multi-state transaction context. For example, it was asked whether the issue of whether a state law was ''contrary to'' should be determined by the law of the state where the treatment is provided, where the claim processor is located, where the payment is issued, or the data maintained, assuming all are in different states.

Response: This is a choice of law issue, and, as is discussed more fully below, is a determination that is routinely made today in connection with multi-state transactions. See discussion below under Exception Determinations (Criteria for Exception Determinations).

State Law

Comment: Comments noted that the definition of ''state law'' does not explicitly include common law and recommended that it be revised to do so or to clarify that the term includes evidentiary privileges recognized at state law. Guidance concerning the impact of state privileges was also requested.

Response: As requested, we clarify that the definition of ''state law'' includes common law by including the term ''common law.'' In our view, this phrase encompasses evidentiary privileges recognized at state law (which may also, we note, be embodied in state statutes).

Comment: One comment criticized this definition as unwieldy, in that locating state laws pertaining to privacy is likely to be difficult. It was noted that Florida, for example, has more than 60 statutes that address health privacy.

Response: To the extent that state laws currently apply to covered entities, they have presumably determined what those laws require in order to comply with them. Thus, while determining which laws are ''contrary'' to the federal requirements will require additional work in terms of comparing state law with the federal requirements, entities should already have acquired the knowledge of state law needed for this task in the ordinary course of doing business.

Comment: The New York City Department of Health noted that in many cases, provisions of New York State law are inapplicable within New York City, because the state legislature has recognized that the local code is tailored to the particular needs of the City. It urged that the New York City Code be treated as state law, for preemption purposes.

Response: We agree that, to the extent a state treats local law as substituting for state law it could be considered to be ''state law'' for purposes of this definition. If, however, a local law is local in scope and effect, and a tier of state law exists over the same subject matter, we do not think that the local law could or should be treated as ''state law'' for preemption purposes. We do not have sufficient information to assess the situation raised by this comment with respect to this principle, and so express no opinion thereon.

More Stringent

Comment: Many commenters supported the policy in the proposed definition of ''individual'' at proposed § 164.502, which would have permitted unemancipated minors to exercise, on

their own behalf, rights granted to individuals in cases where they consented to the underlying health care. Commenters stated, however, that the proposed preemption provision would leave in place state laws authorizing or prohibiting disclosure to parents of the protected health information of their minor children and would negate the proposed policy for the treatment of minors under the rule. The comments stated that such state laws should be treated like other state laws, and preempted to the extent that they are less protective of the privacy of minors.

Other commenters supported the proposed preemption provision—not to preempt a state law to the extent it authorizes or prohibits disclosure of protected health information regarding a minor to a parent.

Response: Laws regarding access to health care for minors and confidentiality of their medical records vary widely; this regulation recognizes and respects the current diversity of state law in this area. Where states have considered the balance involved in protecting the confidentiality of minors' health information and have explicitly acted, for example, to authorize disclosure, defer the decision to disclose to the discretion of the health care provider, or prohibit disclosure of minor's protected health information to a parent, the rule defers to these decisions to the extent that they regulate such disclosures.

Comment: The proposed definition of ''more stringent'' was criticized as affording too much latitude to for granting exceptions for state laws that are not protective of privacy. It was suggested that the test should be ''most protective of the individual's privacy.''

Response: We considered adopting this test. However, for the reasons set out at 64 FR 59997, we concluded that this test would not provide sufficient guidance. The comments did not address the concerns we raised in this regard in the preamble to the proposed rules, and we continue to believe that they are valid.

Comment: A drug company expressed concern with what it saw as the expansive definition of this term, arguing that state governments may have less experience with the special needs of researchers than federal agencies and may unknowingly adopt laws that have a deleterious effect on research. A provider group expressed concern that allowing stronger state laws to prevail could result in diminished ability to get enough patients to complete high quality clinical trials.

Response: These concerns are fundamentally addressed to the ''federal floor'' approach of the statute, not to the definition proposed: even if the definition of ''more stringent'' were narrowed, these concerns would still exist. As discussed above, since the ''federal floor'' approach is statutory, it is not within the Secretary's authority to change the dynamics that are of concern.

Comment: One comment stated that the proposed rule seemed to indicate that the ''more stringent'' and ''contrary to'' definitions implied that these standards would apply to ERISA plans as well as to non-ERISA plans.

Response: The concern underlying this comment is that ERISA plans, which are not now subject to certain state laws because of the ''field'' preemption provision of ERISA but which are subject to the rules below, will become subject to state privacy laws that are ''more stringent'' than the federal requirements, due to the operation of section 1178(a)(2)(B), together with section 264(c)(2). We disagree that this is the case. While the courts will have the final say on these questions, it is our view that these sections simply leave in place more stringent state laws that would otherwise apply; to the extent that such state laws do not apply to ERISA plans because they are preempted by ERISA, we do not think that section 264(c)(2) overcomes the preemption effected by section 514(a) of ERISA. For more discussion of this point, see 64 FR 60001.

Comment: The Lieutenant Governor's Office of the State of Hawaii requested a blanket exemption for Hawaii from the federal rules, on the ground that its recently enacted comprehensive health privacy law is, as a whole, more stringent than the proposed federal standards. It was suggested that, for example, special weight should be given to the severity of Hawaii's penalties. It was suggested that a new definition (''comprehensive'') be added, and that ''more stringent'' be defined in that context as whether the state act or code as a whole provides greater protection.

An advocacy group in Vermont argued that the Vermont legislature was poised to enact stronger and more comprehensive privacy laws and stated that the group would resent a federal prohibition on that.

Response: The premise of these comments appears to be that the provision-by-provision approach of Subpart B, which is expressed in the definition of the term ''contrary'', is wrong. As we explained in the preamble to the proposed rules (at 64 FR 59995), however, the statute dictates a provision-by-provision comparison of state and federal requirements, not the overall comparison suggested by these comments. We also note that the approach suggested would be practically and analytically problematic, in that it would be extremely difficult, if not impossible, to determine what is a legitimate stopping point for the provisions to be weighed on either the state side or the federal side of the scale in determining which set of laws was the ''more stringent.'' We accordingly do not accept the approach suggested by these comments.

With respect to the comment of the Vermont group, nothing in the rules below prohibits or places any limits on states enacting stronger or more comprehensive privacy laws. To the extent that states enact privacy laws that are stronger or more comprehensive than contrary federal requirements, they will presumably not be preempted under section 1178(a)(2)(B). To the extent that such state laws are not contrary to the federal requirements, they will act as an overlay on the federal requirements and will have effect.

Comment: One comment raised the issue of whether a private right of action is a greater penalty, since the proposed federal rule has no comparable remedy.

Response: We have reconsidered the proposed ''penalty'' provision of the proposed definition of ''more stringent'' and have eliminated it. The HIPAA statute provides for only two types of penalties: fines and imprisonment. Both types of penalties could be imposed in addition to the same type of penalty imposed by a state law, and should not interfere with the imposition of other types of penalties that may be available under state law. Thus, we think it is unlikely that there would be a conflict between state and federal law in this respect, so that the proposed criterion is unnecessary and confusing. In addition, the fact that a state law allows an individual to file a lawsuit to protect privacy does not conflict with the HIPAA penalty provisions.

Relates to the Privacy of Individually Identifiable Health Information

Comment: One comment criticized the definition of this term as too narrow in scope and too uncertain. The commenter argued that determining the specific purpose of a state law may be difficult and speculative, because many state laws have incomplete, inaccessible, or non-existent legislative histories. It was suggested that the definition be revised by deleting the word ''specific'' before the word ''purpose.'' Another commenter argued

that the definition of this term should be narrowed to minimize reverse preemption by more stringent state laws. One commenter generally supported the proposed definition of this term.

Response: We are not accepting the first comment. The purpose of a given state enactment should be ascertainable, if not from legislative history or a purpose statement, then from the statute viewed as a whole. The same should be true of state regulations or rulings. In any event, it seems appropriate to restrict the field of state laws that may potentially trump the federal standards to those that are clearly intended to establish state public policy and operate in the same area as the federal standards. To the extent that the definition in the rules below does this, we have accommodated the second comment. We note, however, that we do not agree that the definition should be further restricted to minimize ''reverse preemption,'' as suggested by this comment, as we believe that state laws that are more protective of privacy than contrary federal standards should remain, in order to ensure that the privacy of individuals' health information receives the maximum legal protection available.

Sections 160.203 and 160.204—Exception Determinations and Advisory Opinions

Most of the comments received on proposed Subpart B lumped together the proposed process for exception determinations under section 1178(a)(2)(A) with the proposed process for issuing advisory opinions under section 1178(a)(2)(B), either because the substance of the comment applied to both processes or because the commenters did not draw a distinction between the two processes. We address these general comments in this section.

Comment: Numerous commenters, particularly providers and provider groups, recommended that exception determinations and advisory opinions not be limited to states and advocated allowing all covered entities (including individuals, providers and insurers), or private sector organizations, to request determinations and opinions with respect to preemption of state laws. Several commenters argued that limiting requests to states would deny third party stakeholders, such as life and disability income insurers, any means of resolving complex questions as to what rule they are subject to. One commenter noted that because it is an insurer who will be liable if it incorrectly analyzes the interplay between laws and reaches an incorrect conclusion, there would be little incentive for the states to request clarification. It would also cause large administrative burdens which, it was stated, would be costly and confusing. It was also suggested that the request for the exception be made to the applicable state's attorney general or chief legal officer, as well as the Secretary. Various changes to the language were suggested, such as adding that ''a covered entity, or any other entity impacted by this rule'' be allowed to submit the written request.

Response: We agree, and have changed § 164.204(a) below accordingly.

The decision to eliminate advisory opinions makes this issue moot with respect to those opinions.

Comment: Several commenters noted that it was unclear under the proposed rule which state officials would be authorized to request a determination.

Response: We agree that the proposed rule was unclear in this respect. The final rule clarifies who may make the request for a state, with respect to exception determinations. See, § 160.204(a). The language adopted should ensure that the Secretary receives an authoritative statement from the state. At the same time, this language provides states with flexibility, in that the governor or other chief elected official may choose to designate other state officials to make such requests.

Comment: Many commenters recommended that a process be established whereby HHS performs an initial state-by-state critical analysis to provide guidance on which state laws will not be preempted; most suggested that such an analysis (alternatively referred to as a database or clearinghouse) should be completed before providers would be required to come into compliance. Many of these comments argued that the Secretary should bear the cost for the analyses of state law, disagreeing with the premise stated in the preamble to the proposed rules that it is more efficient for the private market to complete the state-by-state review. Several comments also requested that HHS continue to maintain and monitor the exception determination process, and update the database over time in order to provide guidance and certainty on the interaction of the federal rules with newly enacted or amended state laws that are produced after the final rule. Some comments recommended that each state be required to certify agreement with the HHS analyses.

In contrast, one hospital association noted concerns that the Secretary would conduct a nationwide analysis of state laws. The comment stated that implementation would be difficult since much of the law is a product of common law, and such state-specific research should only be attempted by experienced health care attorneys in each jurisdiction.

Response: These comments seem to be principally concerned with potential conflicts between state privacy laws and the privacy standards, because, as is more fully explained below, preemption of contrary state laws not relating to privacy is automatic unless the Secretary affirmatively acts under section 1178(a)(2)(A) to grant an exception. We recognize that the provisions of sections 1178(b) (state public health laws), and 1178(c) (state regulation of health plans) similarly preserve state laws in those areas, but very little of the public comment appeared to be concerned with these latter statutory provisions. Accordingly, we respond below to what we see as the commenters' main concern.

The Department will not do the kind of global analysis requested by many of these comments. What these comments are in effect seeking is a global advisory opinion as to when the federal privacy standards will control and when they will not. We understand the desire for certainty underlying these comments. Nonetheless, the reasons set out above as the basis for our decision not to establish a formal advisory opinion process apply equally to these requests. We also do not agree that the task of evaluating the requirements below in light of existing state law is unduly burdensome or unreasonable. Rather, it is common for new federal requirements to necessitate an examination by the regulated entities of the interaction between existing state law and the federal requirements incident to coming into compliance.

We agree, however, that the case is different where the Secretary has affirmatively acted, either through granting an exception under section 1178(a)(2)(A) or by making a specific determination about the effect of a particular state privacy law in, for example, the course of determining an entity's compliance with the privacy standards. As is discussed below, the Department intends to make notice of exception determinations that it makes routinely available.

We do not agree with the comments suggesting that compliance by covered entities be delayed pending completion of an analysis by the Secretary and that states be required to certify agreement with the Secretary's analysis, as we are not institutionalizing the advisory opinion/analysis process upon which these comments are predicated.

Furthermore, with respect to the suggestion regarding delaying the compliance date, Congress provided in section 1175(b) of the Act for a delay in when compliance is required to accommodate the needs of covered entities to address implementation issues such as those raised by these comments. With respect to the suggestion regarding requiring states to certify their agreement with the Secretary's analysis, we have no authority to do this.

Comment: Several commenters criticized the proposed provision for annual publication of determinations and advisory opinions in the **Federal Register** as inadequate. They suggested that more frequent notices should be made and the regulation be changed accordingly, to provide for publication either quarterly or within a few days of a determination. A few commenters suggested that any determinations made, or opinions issued, by the Secretary be published on the Department's website within 10 days or a few days of the determination or opinion.

Response: We agree that the proposed provision for annual publication was inadequate and have accordingly deleted it. Subpart B contains no express requirement for publication, as the Department is free to publish its determinations absent such a requirement. It is our intention to publish notice of exception determinations on a periodic basis in the **Federal Register**. We will also consider other avenues of making such decisions publicly available as we move into the implementation process.

Comment: A few commenters argued that the process for obtaining an exception determination or an advisory opinion from the Secretary will result in a period of time in which there is confusion as to whether state or federal law applies. The proposed regulations say that the federal provisions will remain effective until the Secretary makes a determination concerning the preemption issue. This means that, for example, a state law that was enacted and enforced for many years will be preempted by federal law for the period of time during which it takes the Secretary to make a determination. Then if the Secretary determines that the state law is not preempted, the state law will again become effective. Such situations will result in confusion and unintended violations of the law. One of the commenters suggested that requests for exceptions be required only when a challenge is brought against a particular state law, and that a presumption of validity should lie with state laws. Another commenter, however, urged that ''instead of the presumption of preemption, the state laws in question would be presumed to be subject to the exception unless or until the Secretary makes a determination to the contrary.''

Response: It is true that the effect of section 1178(a)(2)(A) is that the federal standards will preempt contrary state law and that such preemption will not be removed unless and until the Secretary acts to grant an exception under that section (assuming, of course, that another provision of section 1178 does not apply). We do not agree, however, that confusion should result, where the issue is whether a given state law has been preempted under section 1178(a)(2)(A). Because preemption is automatic with respect to state laws that do not come within the other provisions of section 1178 (i.e., sections 1178(a)(2)(B), 1178(b), and 1178(c)), such state laws are preempted until the Secretary affirmatively acts to preserve them from preemption by granting an exception under section 1178(a)(2)(A).

We cannot accept the suggestion that a presumption of validity attach to state laws, and that states not be required to request exceptions except in very narrow circumstances. The statutory scheme is the opposite: The statute effects preemption in the section 1178(a)(2)(A) context unless the Secretary affirmatively acts to except the contrary state law in question.

With respect to preemption under sections 1178(b) and 1178(c) (the carve-outs for state public health laws and state regulation of health plans), we do not agree that preemption is likely to be a major cause of uncertainty. We have deferred to Congressional intent by crafting the permissible releases for public health, abuse, and oversight broadly. See, §§ 164.512(b)—(d) below. Since there must first be a conflict between a state law and a federal requirement in order for an issue of preemption to even arise, we think that, as a practical matter, few preemption questions should arise with respect to sections 1178(b) and 1178(c).

With respect to preemption of state privacy laws under section 1178(a)(2)(B), however, we agree that the situation may be more difficult to ascertain, because the Secretary does not determine the preemption status of a state law under that section, unlike the situation with respect to section 1178(a)(2)(A). We have tried to define the term ''more stringent'' to identify and particularize the factors to be considered by courts to those relevant to privacy interests. The more specific (than the statute) definition of this term at § 160.202 below should provide some guidance in making the determination as to which law prevails. Ambiguity in the state of the law might also be a factor to be taken into account in determining whether a penalty should be applied.

Comment: Several comments recommended that exception determinations or advisory opinions encompass a state act or code in its entirety (in lieu of a provision-specific evaluation) if it is considered more stringent as a whole than the regulation. It was argued that since the provisions of a given law are typically interconnected and related, adopting or overriding them on a provision-by-provision basis would result in distortions and/or unintended consequences or loopholes. For example, when a state law includes authorization provisions, some of which are consistent with the federal requirements and some which are not, the cleanest approach is to view the state law as inconsistent with the federal requirements and thus preempted in its entirety. Similarly, another comment suggested that state confidentiality laws written to address the specific needs of individuals served within a discreet system of care be considered as a whole in assessing whether they are as stringent or more stringent than the federal requirements. Another comment requested explicit clarification that state laws with a broader scope than the regulation will be viewed as more stringent and be allowed to stand.

Response: We have not adopted the approach suggested by these comments. As discussed above with respect to the definition of the term ''more stringent,'' it is our view that the statute precludes the approach suggested. We also suggest that this approach ignores the fact that each separate provision of law usually represents a nuanced policy choice to, for example, permit this use or prohibit that disclosure; the aggregated approach proposed would fail to recognize and weigh such policy choices.

Comment: One comment recommended that the final rule: permit requests for exception determinations and advisory opinions as of the date of publication of the final rule, require the Secretary to notify the requestor within a specified short period of time of all additional information needed, and prohibit enforcement action until the Secretary issues a response.

Response: With respect to the first recommendation, we clarify that requests for exception determinations may be made at any time; since the process for issuing advisory opinions has not been adopted, this recommendation is moot as it pertains

to advisory opinions. With respect to the second recommendation, we will undertake to process exception requests as expeditiously as possible, but, for the reasons discussed below in connection with the comments relating to setting deadlines for those determinations, we cannot commit at this time to a ''specified short period of time'' within which the Secretary may request additional information. We see no reason to agree to the third recommendation. Because contrary state laws for which an exception is available only under section 1178(a)(2)(A) will be preempted by operation of law unless and until the Secretary acts to grant an exception, there will be an ascertainable compliance standard for compliance purposes, and enforcement action would be appropriate where such compliance did not occur.

Sections 160.203(a) and 160.204(a)—Exception Determinations

Section 160.203(a)—Criteria for Exception Determinations

Comment: Numerous comments criticized the proposed criteria for their substance or lack thereof. A number of commenters argued that the effectiveness language that was added to the third statutory criterion made the exception so massive that it would swallow the rule. These comments generally expressed concern that laws that were less protective of privacy would be granted exceptions under this language. Other commenters criticized the criteria generally as creating a large loophole that would let state laws that do not protect privacy trump the federal privacy standards.

Response: We agree with these comments. The scope of the statutory criteria is ambiguous, but they could be read so broadly as to largely swallow the federal protections. We do not think that this was Congress's intent. Accordingly, we have added language to most of the statutory criteria clarifying their scope. With respect to the criteria at 1178(a)(2)(A)(i), this clarifying language generally ties the criteria more specifically to the concern with protecting and making more efficient the health care delivery and payment system that underlies the Administrative Simplification provisions of HIPAA, but, with respect to the catch-all provision at section 1178(a)(2)(A)(i)(IV), also requires that privacy interests be balanced with such concerns, to the extent relevant. We require that exceptions for rules to ensure appropriate state regulation of insurance and health plans be stated in a statute or regulation, so that such exceptions will be clearly tied to statements of priorities made by publicly accountable bodies (e.g., through the public comment process for regulations, and by elected officials through statutes). With respect to the criterion at section 1178(a)(2)(A)(ii), we have further delineated what ''addresses controlled substances'' means. The language provided, which builds on concepts at 21 U.S.C. 821 and the Medicare regulations at 42 CFR 1001.2, delineates the area within which the government traditionally regulates controlled substances, both civilly and criminally; it is our view that HIPAA was not intended to displace such regulation.

Comment: Several commenters urged that the request for determination by the Secretary under proposed § 160.204(a) be limited to cases where an exception is absolutely necessary, and that in making such a determination, the Secretary should be required to make a determination that the benefits of granting an exception outweigh the potential harm and risk of disclosure in violation of the regulation.

Response: We have not further defined the statutory term ''necessary'', as requested. We believe that the determination of what is ''necessary'' will be fact-specific and context dependent, and should not be further circumscribed absent such specifics. The state will need to make its case that the state law in question is sufficiently ''necessary'' to accomplish the particular statutory ground for exception that it should trump the contrary federal standard, requirement, or implementation specification.

Comment: One commenter noted that a state should be required to explain whether it has taken any action to correct any less stringent state law for which an exception has been requested. This commenter recommended that a section be added to proposed § 160.204(a) stating that ''a state must specify what, if any, action has been taken to amend the state law to comply with the federal regulations.'' Another comment, received in the Transactions rulemaking, took the position that exception determinations should be granted only if the state standards in question exceeded the national standards.

Response: The first and last comments appear to confuse the ''more stringent'' criterion that applies under section 1178(a)(2)(B) of the Act with the criteria that apply to exceptions under section 1178(a)(2)(A). We are also not adopting the language suggested by the first comment, because we do not agree that states should necessarily have to try to amend their state laws as a precondition to requesting exceptions under section 1178(a)(2)(A). Rather, the question should be whether the state has made a convincing case that the state law in question is sufficiently necessary for one of the statutory purposes that it should trump the contrary federal policy.

Comment: One commenter stated that exceptions for state laws that are contrary to the federal standards should not be preempted where the state and federal standards are found to be equal.

Response: This suggestion has not been adopted, as it is not consistent with the statute. With respect to the administrative simplification standards in general, it is clear that the intent of Congress was to preempt contrary state laws except in the limited areas specified as exceptions or carve-outs. See, section 1178. This statutory approach is consistent with the underlying goal of simplifying health care transactions through the adoption of uniform national standards. Even with respect to state laws relating to the privacy of medical information, the statute shields such state laws from preemption by the federal standards only if they are ''more'' stringent than the related federal standard or implementation specification.

Comment: One commenter noted that determinations would apply only to transactions that are wholly intrastate. Thus, any element of a health care transaction that would implicate more than one state's law would automatically preclude the Secretary's evaluation as to whether the laws were more or less stringent than the federal requirement. Other commenters expressed confusion about this proposed requirement, noting that providers and plans operate now in a multi-state environment.

Response: We agree with the commenters and have dropped the proposed requirement. As noted by the commenters, health care entities now typically operate in a multi-state environment, so already make the choice of law judgements that are necessary in multi-state transactions. It is the result of that calculus that will have to be weighed against the federal standards, requirements, and implementation specifications in the preemption analysis.

Comment: One comment received in the Transactions rulemaking suggested that the Department should allow exceptions to the standard transactions to accommodate abbreviated transactions between state agencies, such as claims between a public health department and the state Medicaid

agency. Another comment requested an exception for Home and Community Based Waiver Services from the transactions standards.

Response: The concerns raised by these comments would seem to be more properly addressed through the process established for maintaining and modifying the transactions standards. If the concerns underlying these comments cannot be addressed in this manner, however, there is nothing in the rules below to preclude states from requesting exceptions in such cases. They will then have to make the case that one or more grounds for exception applies.

Section 160.204(a)—Process for Exception Determinations—Comments and Responses

Comment: Several comments received in the Transactions rulemaking stated that the process for applying for and granting exception determinations (referred to as ''waivers'' by some) needed to be spelled out in the final rule.

Response: We agree with these comments. As noted above, since no process was proposed in the Transactions rulemaking, a process for making exception determinations was not adopted in those final rules. Subpart B below adopts a process for making exception determinations, which responds to these comments.

Comment: Comments stated that the exception process would be burdensome, unwieldy, and time-consuming for state agencies as well as the Department. One comment took the position that states should not be required to submit exception requests to the Department under proposed § 160.203(a), but could provide documentation that the state law meets one of the conditions articulated in proposed § 160.203.

Response: We disagree that the process adopted at § 164.204 below will be burdensome, unwieldy, or time-consuming. The only thing the regulation describes is the showings that a requestor must make as part of its submission, and all are relevant to the issue to be determined by the Secretary. How much information is submitted is, generally speaking, in the requestor's control, and the regulation places no restrictions on how the requestor obtains it, whether by acting directly, by working with providers and/or plans, or by working with others. With respect to the suggestion that states not be required to submit exception requests, we disagree that this suggestion is either statutorily authorized or advisable. We read this comment as implicitly suggesting that the Secretary must proactively identify instances of conflict and evaluate them. This suggestion is, thus, at bottom the same as the many suggestions that we create a database or compendium of controlling law, and it is rejected for the same reasons.

Comment: Several comments urged that all state requests for non-preemption include a process for public participation. These comments believe that members of the public and other interested stakeholders should be allowed to submit comments on a state's request for exception, and that these comments should be reviewed and considered by the Secretary in determining whether the exception should be granted. One comment suggested that the Secretary at least give notice to the citizens of the state prior to granting an exception.

Response: The revision to § 160.204(a), to permit requests for exception determinations by any person, responds to these comments.

Comment: Many commenters noted that the lack of a clear and reasonable time line for the Secretary to issue an exception determination would not provide sufficient assurance that the questions regarding what rules apply will be resolved in a time frame that will allow business to be conducted properly, and argued that this would increase confusion and uncertainty about which statutes and regulations should be followed. Timeframes of 60 or 90 days were suggested. One group suggested that, if a state does not receive a response from HHS within 60 days, the waiver should be deemed approved.

Response: The workload prioritization and management considerations discussed above with respect to advisory opinions are also relevant here and make us reluctant to agree to a deadline for making exception determinations. This is particularly true at the outset, since we have no experience with such requests. We therefore have no basis for determining how long processing such requests will take, how many requests we will need to process, or what resources will be available for such processing. We agree that states and other requesters should receive timely responses and will make every effort to make determinations as expeditiously as possible, but we cannot commit to firm deadlines in this initial rule. Once we have experience in handling exception requests, we will consult with states and others in regard to their experiences and concerns and their suggestions for improving the Secretary's expeditious handling of such requests.

We are not accepting the suggestion that requests for exception be deemed approved if not acted upon in some defined time period. Section 1178(a)(2)(A) requires a specific determination by the Secretary. The suggested policy would not be consistent with this statutory requirement. It is also inadvisable from a policy standpoint, in that it would tend to maximize exceptions. This would be contrary to the underlying statutory policy in favor of uniform federal standards.

Comment: One commenter took exception to the requirement for states to seek a determination from the Department that a provision of state law is necessary to prevent fraud and abuse or to ensure appropriate state regulation of insurance plans, contending that this mandate could interfere with the Insurance Commissioners' ability to do their jobs. Another commenter suggested that the regulation specifically recognize the broad scope of state insurance department activities, such as market conduct examinations, enforcement investigations, and consumer complaint handling.

Response: The first comment raises an issue that lies outside our legal authority to address, as section 1178(a)(2)(A) clearly mandates that the Secretary make a determination in these areas. With respect to the second comment, to the extent these concerns pertain to health plans, we believe that the provisions at § 164.512 relating to oversight and disclosures required by law should address the concerns underlying this comment.

Section 160.204(a)(4)—Period of Effectiveness of Exception Determinations

Comment: Numerous commenters stated that the proposed three year limitation on the effectiveness of exception determinations would pose significant problems and should be limited to one year, since a one year limitation would provide more frequent review of the necessity for exceptions. The commenters expressed concern that state laws which provide less privacy protection than the federal regulation would be given exceptions by the Secretary and thus argued that the exceptions should be more limited in duration or that the Secretary should require that each request, regardless of duration, include a description of the length of time such an exception would be needed.

One state government commenter, however, argued that the 3 year limit should be eliminated entirely, on the ground that requiring a redetermination

every three years would be burdensome for the states and be a waste of time and resources for all parties. Other commenters, including two state agencies, suggested that the exemption should remain effective until either the state law or the federal regulation is changed. Another commenter suggested that the three year sunset be deleted and that the final rule provide for automatic review to determine if changes in circumstance or law would necessitate amendment or deletion of the opinion. Other recommendations included deeming the state law as continuing in effect upon the submission of a state application for an exemption rather than waiting for a determination by the Secretary that may not occur for a substantial period of time.

Response: We are persuaded that the proposed 3 year limit on exception determinations does not make sense where neither law providing the basis for the exception has changed in the interim. We also agree that where either law has changed, a previously granted exception should not continue. Section 160.205(a) below addresses these concerns.

Sections 160.203(b) and 160.204(b)—Advisory Opinions

Section 160.203(b)—Effect of Advisory Opinions

Comment: Several commenters questioned whether or not DHHS has standing to issue binding advisory opinions and recommended that the Department clarify this issue before implementation of this regulation. One respondent suggested that the Department clarify in the final rule the legal issues on which it will opine in advisory opinion requests, and state that in responding to requests for advisory opinions the Department will not opine on the preemptive force of ERISA with respect to state laws governing the privacy of individually identifiable health information, since interpretations as to the scope and extent of ERISA's preemption provisions are outside of the Department's jurisdictional authority.

One commenter asked whether a state could enforce a state law which the Secretary had indicated through an advisory opinion is preempted by federal law. This commenter also asked whether the state would be subject to penalties if it chose to continue to enforce its own laws.

Response: As discussed above, in part for reasons raised by these comments, the Department has decided not to have a formal process for issuing advisory opinions, as proposed.

Several of these concerns, however, raise issues of broader concern that need to be addressed. First, we disagree that the Secretary lacks legal authority to opine on whether or not state privacy laws are preempted. The Secretary is charged by law with determining compliance, and where state law and the federal requirements conflict, a determination of which law controls will have to be made in order to determine whether the federal standard, requirement, or implementation specification at issue has been violated. Thus, the Secretary cannot carry out her enforcement functions without making such determinations. It is further reasonable that, if the Secretary makes such determinations, she can make those determinations known, for whatever persuasive effect they may have.

The questions as to whether a state could enforce, or would be subject to penalties if it chose to continue to enforce, its own laws following a denial by the Secretary of an exception request under § 160.203 or a holding by a court of competent jurisdiction that a state privacy law had been preempted by a contrary federal privacy standard raise several issues. First, a state law is preempted under the Act only to the extent that it applies to covered entities; thus, a state is free to continue to enforce a ''preempted'' state law against non-covered entities to which the state law applies. If there is a question of coverage, states may wish to establish processes to ascertain which entities within their borders are covered entities within the meaning of these rules. Second, with respect to covered entities, if a state were to try to enforce a preempted state law against such entities, it would presumably be acting without legal authority in so doing. We cannot speak to what remedies might be available to covered entities to protect themselves against such wrongful state action, but we assume that covered entities could seek judicial relief, if all else failed. With respect to the issue of imposing penalties on states, we do not see this as likely. The only situation that we can envision in which penalties might be imposed on a state would be if a state agency were itself a covered entity and followed a preempted state law, thereby violating the contrary federal standard, requirement, or implementation specification.

Section 160.204(b)—Process for Advisory Opinions

Comment: Several commenters stated that it was unclear whether a state would be required to submit a request for an advisory opinion in order for the law to be considered more stringent and thus not preempted. The Department should clarify whether a state law could be non-preempted even without such an advisory opinion. Another commenter requested that the final rule explicitly state that the stricter rule always applies, whether it be state or federal, and regardless of whether there is any conflict between state and federal law.

Response: The elimination of the proposed process for advisory opinions renders moot the first question. Also, the preceding response clarifies that which law preempts in the privacy context (assuming that the state law and federal requirement are ''contrary'') is a matter of which one is the ''more stringent.'' This is not a matter which the Secretary will ultimately determine; rather, this is a question about which the courts will ultimately make the final determination. With respect to the second comment, we believe that § 160.203(b) below responds to this issue, but we would note that the statute already provides for this.

Comment: Several commenters supported the decision to limit the parties who may request advisory opinions to the state. These commenters did not believe that insurers should be allowed to request an advisory opinion and open every state law up to challenge and review.

Several commenters requested that guidance on advisory opinions be provided in *all* circumstances, not only at the Secretary's discretion. It was suggested that proposed § 160.204(b)(2)(iv) be revised to read as follows: ''A state may submit a written request to the Secretary for an advisory opinion under this paragraph. The request must include the following information: the reasons why the state law *should* or *should not be* preempted by the federal standard, requirement, or implementation specification, including how the state law meets the criteria at § 160.203(b).''

Response: The decision not to have a formal process for issuing advisory opinions renders these issues moot.

Sections 160.203(c) and 160.203(d)—Statutory Carve-Outs

Comment: Several commenters asked that the Department provide more specific examples itemizing activities traditionally regulated by the state that could constitute ''carve-out'' exceptions. These commenters also requested that the Department include language in the regulation stating that if a state law falls within several different exceptions, the state chooses which determination exception shall apply.

Response: We are concerned that itemizing examples in this way could leave out important state laws or create inadvertent negative implications that laws not listed are not included. However, as explained above, we have designed the types of activities that are permissive disclosures for public health under § 164.512(b) below in part to come within the carve-out effected by section 1178(b); while the state regulatory activities covered by section 1178(c) will generally come within § 164.512(d) below. With respect to the comments asking that a state get to ''choose'' which exception it comes under, we have in effect provided for this with respect to exceptions under section 1178(a)(2)(A), by giving the state the right to request an exception under that section. With respect to exceptions under section 1178(a)(2)(B), those exceptions occur by operation of law, and it is not within the Secretary's power to ''let'' the state choose whether an exception occurs under that section.

Comment: Several commenters took the position that the Secretary should not limit the procedural requirements in proposed § 160.204(a) to only those applications under proposed § 160.203(a). They urged that the requirements of proposed § 160.204(a) should also apply to preemption under sections 1178(a)(2)(B), 1178(b) and 1178(c). It was suggested that the rules should provide for exception determinations with respect to the matters covered by these provisions of the statute; such additional provisions would provide clear procedures for states to follow and ensure that requests for exceptions are adequately documented.

A slightly different approach was taken by several commenters, who recommended that proposed § 160.204(b) be amended to clarify that the Secretary will also issue advisory opinions as to whether a state law constitutes an exception under proposed §§ 160.203(c) and 160.203(d). This change would, they argued, give states the same opportunity for guidance that they have under § 160.203(a) and (b), and as such, avoid costly lawsuits to preserve state laws.

Response: We are not taking either of the recommended courses of action. With respect to the recommendation that we expand the exception determination process to encompass exceptions under sections 1178(a)(2)(B), 1178(b), and 1178(c), we do not have the authority to grant exceptions under these sections. Under section 1178, the Secretary has authority to make exception determinations only with respect to the matters covered by section 1178(a)(2)(A); contrary state laws coming within section 1178(a)(2)(B) are preempted if not more stringent, while if a contrary state law comes within section 1178(b) or section 1178(c), it is not preempted. These latter statutory provisions operate by their own terms. Thus, it is not within the Secretary's authority to establish the determination process which these comments seek.

With respect to the request seeking advisory opinions in the section 1178(b) and 1178(c) situations, we agree that we have the authority to issue such opinions. However, the considerations described above that have led us not to adopt a formal process for issuing advisory opinions in the privacy context apply with equal force and effect here.

Comment: One commenter argued that it would be unnecessarily burdensome for state health data agencies (whose focus is on the cost of healthcare or improving Medicare, Medicaid, or the healthcare system) to obtain a specific determination from the Department for an exception under proposed § 160.203(c). States should be required only to notify the Secretary of their own determination that such collection is necessary. It was also argued that cases where the statutory carve-outs apply should not require a Secretarial determination.

Response: We clarify that no Secretarial determination is required for activities that fall into one of the statutory carve-outs. With respect to data collections for state health data agencies, we note that provision has been made for many of these activities in several provisions of the rules below, such as the provisions relating to disclosures required by law (§ 164.512(a)), disclosures for oversight (§ 164.512(d)), and disclosures for public health (§ 164.512(b)). Some disclosures for Medicare and Medicaid purposes may also come within the definition of health care operations. A fuller discussion of this issue appears in connection with § 164.512 below.

Constitutional Comments and Responses

Comment: Several commenters suggested that as a general matter the rule is unconstitutional.

Response: We disagree that the rule is unconstitutional. The particular grounds for this conclusion are set out with respect to particular constitutional issues in the responses below. With respect to the comments that simply made this general assertion, the lack of detail of the comments makes a substantive response impossible.

Article II

Comment: One commenter contended that the Secretary improperly delegated authority to private entities by requiring covered entities to enter into contracts with, monitor, and take action for violations of the contract against their business partners. These comments assert that the selection of these entities to ''enforce'' the regulations violates the Executive Powers Clause and the Appointments and Take Care Clauses.

Response: We reject the assertion that the business associate provisions constitute an improper delegation of executive power to private entities. HIPAA provides HHS with authority to enforce the regulation against covered entities. The rules below regulate only the conduct of the covered entity; to the extent a covered entity chooses to conduct its funding through a business associate, those functions are still functions of the covered entity. Thus, no improper delegation has occurred because what is being regulated are the actions of the covered entity, not the actions of the business associate in its independent capacity.

We also reject the suggestion that the business associates provisions constitute an improper appointment of covered entities to enforce the regulation and violate the Take Care Clause. Because the Secretary has not delegated authority to covered entities, the inference that she has appointed covered entities to exercise such authority misses the mark.

Commerce Clause

Comment: A few commenters suggested that the privacy regulation regulates activities that are not in interstate commerce and which are, therefore, beyond the powers the U.S. Constitution gives the federal government.

Response: We disagree. Health care providers, health plans, and health care clearinghouses are engaged in economic and commercial activities, including the exchange of individually identifiable health information electronically across state lines. These activities constitute interstate commerce. Therefore, they come within the scope of Congress' power to regulate interstate commerce.

Nondelegation Doctrine

Comment: Some commenters objected to the manner by which Congress provided the Secretary authority to promulgate this regulation. These comments asserted that Congress violated the nondelegation doctrine by (1) not providing an ''intelligible principle'' to guide the agency, (2) not

establishing ''ascertainable standards,'' and (3) improperly permitting the Secretary to make social policy decisions.

Response: We disagree. HIPAA clearly delineates Congress' general policy to establish strict privacy protections for individually identifiable health information to encourage electronic transactions. Congress also established boundaries limiting the Secretary's authority. Congress established these limitations in several ways, including by calling for privacy standards for ''individually identifiable health information''; specifying that privacy standards must address individuals' rights regarding their individually identifiable health information, the procedures for exercising those rights, and the particular uses and disclosures to be authorized or required; restricting the direct application of the privacy standards to ''covered entities,'' which Congress defined; requiring consultation with the National Committee on Vital and Health Statistics and the Attorney General; specifying the circumstances under which the federal requirements would supersede state laws; and specifying the civil and criminal penalties the Secretary could impose for violations of the regulation. These limitations also serve as ''ascertainable standards'' upon which reviewing courts can rely to determine the validity of the exercise of authority.

Although Congress could have chosen to impose expressly an exhaustive list of specifications that must be met in order to achieve the protective purposes of the HIPAA, it was entirely permissible for Congress to entrust to the Secretary the task of providing these specifications based on her experience and expertise in dealing with these complex and technical matters.

We disagree with the comments that Congress improperly delegated Congressional policy choices to her. Congress clearly decided to create federal standards protecting the privacy of ''individually identifiable health information'' and not to preempt state laws that are more stringent. Congress also determined over whom the Secretary would have authority, the type of information protected, and the minimum level of regulation.

Separation of Powers

Comment: Some commenters asserted that the federal government may not preempt state laws that are not as strict as the privacy regulation because to do so would violate the separation of powers in the U.S. Constitution. One comment suggested that the rules raised a substantial constitutional issue because, as proposed, they permitted the Secretary to make determinations on preemption, which is a role reserved for the judiciary.

Response: We disagree. We note that this comment only pertains to determinations under section 1178(a)(2)(A); as discussed above, the rules below provide for no Secretarial determinations with respect to state privacy laws coming within section 1178(a)(2)(B). With respect to determinations under section 1178(a)(2)(A), however, the final rules, like the proposed rules, provide that at a state's request the Secretary may make certain determinations regarding the preemptive effect of the rules on a particular state law. As usually the case with any administrative decisions, these are subject to judicial review pursuant to the Administrative Procedure Act.

First Amendment

Comment: Some comments suggested that the rules violated the First Amendment. They asserted that if the rule included Christian Science practitioners as covered entities it would violate the separation of church and state doctrine.

Response: We disagree. The First Amendment does not always prohibit the federal government from regulating secular activities of religious organizations. However, we address concerns relating to Christian Science practitioners more fully in the response to comments discussion of the definition of ''covered entity'' in § 160.103.

Fourth Amendment

Comment: Many comments expressed Fourth Amendment concerns about various proposed provisions. These comments fall into two categories—general concerns about warrantless searches and specific concerns about administrative searches. Several comments argued that the proposed regulations permit law enforcement and government officials access to protected health information without first requiring a judicial search warrant or an individual's consent. These comments rejected the applicability of any of the existing exceptions permitting warrantless searches in this context. Another comment argued that federal and state police should be able to obtain personal medical records only with the informed consent of an individual. Many of these comments also expressed concern that protected health information could be provided to government or private agencies for inclusion in a governmental health data system.

Response: We disagree that the provisions of these rules that permit disclosures for law enforcement purposes and governmental health data systems generally violate the Fourth Amendment. The privacy regulation does not create new access rights for law enforcement. Rather, it refrains from placing a significant barrier in front of access rights that law enforcement currently has under existing legal authority. While the regulation may permit a covered entity to make disclosures in specified instances, it does not require the covered entity make the disclosure. Thus, because we are not modifying existing law regarding disclosures to law enforcement officials, except to strengthen the requirements related to requests already authorized under law, and are not requiring any such disclosures, the privacy regulation does not infringe upon individual's Fourth Amendment rights. We discuss the rationale underlying the permissible disclosures to law enforcement officials more fully in the preamble discussion relating to § 164.512(f).

We note that the proposed provision relating to disclosures to government health data systems has been eliminated in the final rule. However, to the extent that the comments can be seen as raising concern over disclosure of protected health information to government agencies for public health, health oversight, or other purposes permitted by the final rule, the reasoning in the previous paragraph applies.

Comment: One commenter suggested that the rules violate the Fourth Amendment by requiring covered entities to provide access to the Secretary to their books, records, accounts, and facilities to ensure compliance with these rules. The commenter also suggested that the requirement that covered entities enter into agreements with their business partners to make their records available to the Secretary for inspection as well also violates the warrant requirement of the Fourth Amendment.

Response: We disagree. These requirements are consistent with U.S. Supreme Court cases holding that warrantless administrative searches of commercial property are not per se violations of the Fourth Amendment. The provisions requiring that covered entities provide access to certain material to determine compliance with the regulation come within the well-settled exception regarding closely regulated businesses and industries to the warrant requirement. From state and local licensure laws to the federal fraud and abuse statutes and regulations, the health care industry is one of the most

tightly regulated businesses in the country. Because the industry has such an extensive history of government oversight and involvement, those operating within it have no reasonable expectation of privacy from the government such that a warrant would be required to determine compliance with the rules.

In addition, the cases cited by the commenters concern unannounced searches of the premises and facilities of particular entities. Because our enforcement provisions only provide for the review of books, records, and other information and only during normal business hours with notice, except for exceptional situations, this case law does not apply.

As for business associates, they voluntarily enter into their agreements with covered entities. This agreement, therefore, functions as knowing and voluntary consents to the search (even assuming it could be understood to be a search) and obviates the need for a warrant.

Fifth Amendment

Comment: Several comments asserted that the proposed rules violated the Fifth Amendment because in the commenters' views they authorized the taking of privacy property without just compensation or due process of law.

Response: We disagree. The rules set forth below do not address the issue of who owns an individual's medical record. Instead, they address what uses and disclosures of protected health information may be made by covered entities with or without a consent or authorization. As described in response to a similar comment, medical records have been the property of the health care provider or medical facility that created them, historically. In some states, statutes directly provide these entities with ownership. These laws are limited by laws that provide patients or their representatives with access to the records or that provide the patient with an ownership interest in the information within the records. As we discuss, the final rule is consistent with current state law that provides patients access to protected health information, but not ownership of medical records. State laws that provide patients with greater access would remain in effect. Therefore, because patients do not own their records, no taking can occur. As for their interest in the information, the final rule retains their rights. As for covered entities, the final rule does not take away their ownership rights or make their ownership interest in the protected health information worthless. Therefore, no taking has occurred in these situations either.

Ninth and Tenth Amendments

Comment: Several comments asserted that the proposed rules violated the Ninth and Tenth Amendments. One commenter suggested that the Ninth Amendment prohibits long and complicated regulations. Other commenters suggested that the proposed rules authorized the compelled disclosure of individually identifiable health information in violation of State constitutional provisions, such as those in California and Florida. Similarly, a couple of commenters asserted that the privacy rules violate the Tenth Amendment.

Response: We disagree. The Ninth and Tenth Amendments address the rights retained by the people and acknowledge that the States or the people are reserved the powers not delegated to the federal government and not otherwise prohibited by the Constitution. Because HHS is regulating under a delegation of authority from Congress in an area that affects interstate commerce, we are within the powers provided to Congress in the Constitution. Nothing in the Ninth Amendment, or any other provision of the Constitution, restricts the length or complexity of any law. Additionally, we do not believe the rules below impermissibly authorize behavior that violates State constitutions. This rule requires disclosure only to the individual or to the Secretary to enforce this rule. As noted in the preamble discussion of ''Preemption,'' these rules do not preempt State laws, including constitutional provisions, that are contrary to and more stringent, as defined at § 160.502, than these rules. See the discussion of ''Preemption'' for further clarification. Therefore, if these State constitutions are contrary to the rule below and provide greater protection, they remain in full force; if they do not, they are preempted, in accordance with the Supremacy Clause of the Constitution.

Right to Privacy

Comment: Several comments suggested that the proposed regulation would violate the right to privacy guaranteed by the First, Fourth, Fifth, and Ninth Amendments because it would permit covered entities to disclose protected health information without the consent of the individual.

Response: These comments did not provide specific facts or legal basis for the claims. We are, thus, unable to provide a substantive response to these particular comments. However, we note that the rule requires disclosures only to the individual or to the Secretary to determine compliance with this rule. Other uses or disclosures under this rule are permissive, not required. Therefore, if a particular use or disclosure under this rule is viewed as interfering with a right that prohibited the use or disclosure, the rule itself is not what requires the use or disclosure.

Void for Vagueness

Comment: One comment suggested that the Secretary's use of a ''reasonableness'' standard is unconstitutionally vague. Specifically, this comment objected to the requirement that covered entities use ''reasonable'' efforts to use or disclose the minimum amount of protected health information, to ensure that business partners comply with the privacy provisions of their contracts, to notify business partners of any amendments or corrections to protected health information, and to verify the identity of individuals requesting information, as well as charge only a ''reasonable'' fee for inspecting and copying health information. This comment asserted that the Secretary provided ''inadequate guidance'' as to what qualifies as ''reasonable.''

Response: We disagree with the comment's suggestion that by applying a ''reasonableness'' standard, the regulation has failed to provide for ''fair warning'' or ''fair enforcement.'' The ''reasonableness'' standard is well-established in law; for example, it is the foundation of the common law of torts. Courts also have consistently held as constitutional statutes that rely upon a ''reasonableness'' standard. Our reliance upon a ''reasonableness'' standard, thus, provides covered entities with constitutionally sufficient guidance.

Criminal Intent

Comment: One comment argued that the regulation's reliance upon a ''reasonableness'' standard criminalizes ''unreasonable efforts'' without requiring criminal intent or *mens rea.*

Response: We reject this suggestion because HIPAA clearly provides the criminal intent requirement. Specifically, HIPPA provides that a ''person who knowingly and in violation of this part—(1) uses or causes to be used a unique health identifier; (2) obtains individually identifiable health information relating to an individual; or (3) discloses individually identifiable health information to another person, shall be punished as provided in subsection (b).'' HIPAA section 1177 (emphasis added). Subsection (b) also relies on a knowledge standard in

outlining the three levels of criminal sanctions. Thus, Congress, not the Secretary, established the *mens rea* by including the term ''knowingly'' in the criminal penalty provisions of HIPAA.

Data Collection

Comment: One commenter suggested that the U.S. Constitution authorized the collection of data on individuals only for the purpose of the census.

Response: While it might be true that the U.S. Constitution expressly discusses the national census, it does not forbid federal agencies from collecting data for other purposes. The ability of agencies to collect non-census data has been upheld by the courts.

Relationship to Other Federal Laws

Comment: We received several comments that sought clarification of the interaction of various federal laws and the privacy regulation. Many of these comments simply listed federal laws and regulations with which the commenter currently must comply. For example, commenters noted that they must comply with regulations relating to safety, public health, and civil rights, including Medicare and Medicaid, the Americans with Disabilities Act, the Family and Medical Leave Act, the Federal Aviation Administration regulations, the Department of Transportation regulations, the Federal Highway Administration regulations, the Occupational Safety and Health Administration regulations, and the Environmental Protection Agency regulations, and alcohol and drug free workplace rules. These commenters suggested that the regulation state clearly and unequivocally that uses or disclosures of protected health information for these purposes were permissible. Some suggested modifying the definition of health care operations to include these uses specifically. Another suggestion was to add a section that permitted the transmission of protected health information to employers when reasonably necessary to comply with federal, state, or municipal laws and regulations, or when necessary for public or employee safety and health.

Response: Although we sympathize with entities' needs to evaluate the existing laws with which they must comply in light of the requirements of the final regulation, we are unable to respond substantially to comments that do not pose specific questions. We offer, however, the following guidance: if an covered entity is required to disclose protected health information pursuant to a specific statutory or regulatory scheme, the covered entity generally will be permitted under § 164.512(a) to make these disclosures without a consent or authorization; if, however, a statute or regulation merely suggests a disclosure, the covered entity will need to determine if the disclosure comes within another category of permissible disclosure under §§ 164.510 or 164.512 or, alternatively, if the disclosure would otherwise come within § 164.502. If not, the entity will need to obtain a consent or authorization for the disclosure.

Comment: One commenter sought clarification as to when a disclosure is considered to be ''required'' by another law versus ''permitted'' by that law.

Responses: We use these terms according to their common usage. By ''required by law,'' we mean that a covered entity has a legal obligation to disclose the information. For example, if a statute states that a covered entity must report the names of all individuals presenting with gun shot wounds to the emergency room or else be fined $500 for each violation, a covered entity would be required by law to disclose the protected health information necessary to comply with this mandate. The privacy regulation permits this type of disclosure, but does not require it. Therefore, if a covered entity chose not to comply with the reporting statute it would violate only the reporting statute and not the privacy regulation.

On the other hand, if a statute stated that a covered entity may or is permitted to report the names of all individuals presenting with gun shot wounds to the emergency room and, in turn, would receive $500 for each month it made these reports, a covered entity would not be permitted by § 164.512(a) to disclose the protected health information. Of course, if another permissible provision applied to these facts, the covered entity could make the disclosure under that provision, but it would not be considered to be a disclosure. See discussion under § 164.512(a) below.

Comment: Several commenters suggested that the proposed rule was unnecessarily duplicative of existing regulations for federal programs, such as Medicare, Medicaid, and the Federal Employee Health Benefit Program.

Response: Congress specifically subjected certain federal programs, including Medicare, Medicaid, and the Federal Employee Health Benefit Program to the privacy regulation by including them within the definition of ''health plan.'' Therefore, covered entities subject to requirements of existing federal programs will also have to comply with the privacy regulation.

Comment: One comment asserts that the regulation would not affect current federal requirements if the current requirements are weaker than the requirements of the privacy regulation. This same commenter suggested that current federal requirements will trump both state law and the proposed regulation, even if Medicaid transactions remain wholly intrastate.

Response: We disagree. As noted in our discussion of ''Relationship to Other Federal Laws,'' each law or regulation will need to be evaluated individually. We similarly disagree with the second assertion made by the commenter. The final rule will preempt state laws only in specific instances. For a more detailed analysis, see the preamble discussion of ''Preemption.''

Administrative Subpoenas

Comment: One comment stated that the final rule should not impose new standards on administrative subpoenas that would conflict with existing laws or administrative or judicial rules that establish standards for issuing subpoenas. Nor should the final rule conflict with established standards for the conduct of administrative, civil, or criminal proceedings, including the rules regarding the discovery of evidence. Other comments sought further restrictions on access to protected health information in this context.

Response: Section 164.512(e) below addresses disclosures for judicial and administrative proceedings. The final rules generally do not interfere with these existing processes to the extent an individual served with a subpoena, court order, or other similar process is able to raise objections already available. See the discussion below under § 164.512(e) for a fuller response.

Americans with Disabilities Act

Comment: Several comments discussed the intersection between the proposed Privacy Rule and the Americans with Disabilities Act (''ADA'') and sections 503 and 504 of the Rehabilitation Act of 1973. One comment suggested that the final rule explicitly allows disclosures authorized by the Americans with Disabilities Act without an individual's authorization, because this law, in the commenter's view, provides more than adequate protection for the confidentiality of medical records in the employment context. The comment noted that under these laws employers may receive information related to fitness for duty, pre-employment physicals, routine examinations, return to work examinations, examinations following other types of absences, examinations triggered by specific events, changes in

circumstances, requests for reasonable accommodations, leave requests, employee wellness programs, and medical monitoring.

Other commenters suggested that the ADA requires the disclosure of protected health information to employers so that the employee may take advantage of the protections of these laws. They suggested that the final rules clarify that employment may be conditioned on obtaining an authorization for disclosure of protected health information for lawful purposes and provide guidance concerning the interaction of the ADA with the final regulation's requirements. Several commenters wanted clarification that the privacy regulation would not permit employers to request or use protected health information in violation of the ADA.

Response: We disagree with the comment that the final rule should allow disclosures of protected health information authorized by the ADA without the individual's authorization. We learned from the comments that access to and use of protected health information by employers is of particular concern to many people. With regard to employers, we do not have statutory authority to regulate them. Therefore, it is beyond the scope of this regulation to prohibit employers from requesting or obtaining protected health information. Covered entities may disclose protected health information about individuals who are members of an employer's workforce with an authorization. Nothing in the privacy regulation prohibits employers from obtaining that authorization as a condition of employment. We note, however, that employers must comply with other laws that govern them, such as nondiscrimination laws. For example, if an employer receives a request for a reasonable accommodation, the employer may require reasonable documentation about the employee's disability and the functional limitations that require the reasonable accommodation, if the disability and the limitations are not obvious. If the individual provides insufficient documentation and does not provide the missing information in a timely manner after the employer's subsequent request, the employer may require the individual to go to an appropriate health professional of the employer's choice. In this situation, the employee does not authorize the disclosure of information to substantiate the disability and the need for reasonable accommodation, the employer need not provide the accommodation.

We agree that this rule does not permit employers to request or use protected health information in violation of the ADA or other antidiscrimination laws.

Appropriations Laws

Comment: One comment suggested that the penalty provisions of HIPAA, if extended to the privacy regulation, would require the Secretary to violate ''Appropriations Laws'' because the Secretary could be in the position of assessing penalties against her own and other federal agencies in their roles as covered entities. Enforcing penalties on these entities would require the transfer of agency funds to the General Fund.

Response: We disagree. Although we anticipate achieving voluntary compliance and resolving any disputes prior to the actual assessment of penalties, the Department of Justice's Office of Legal Counsel has determined in similar situations that federal agencies have authority to assess penalties against other federal agencies and that doing so is not in violation of the Anti-Deficiency Act, 31 U.S.C. 1341.

Balanced Budget Act of 1997

Comment: One comment expressed concern that the regulation would place tremendous burdens on providers already struggling with the effects of the Balanced Budget Act of 1997.

Response: We appreciate the costs covered entities face when complying with other statutory and regulatory requirements, such as the Balanced Budget Act of 1997. However, HHS cannot address the impact of the Balanced Budget Act or other statutes in the context of this regulation.

Comment: Another comment stated that the regulation is in direct conflict with the Balanced Budget Act of 1997 (''BBA''). The comment asserts that the regulation's compliance date conflicts with the BBA, as well as Generally Acceptable Accounting Principles. According to the comment, covered entities that made capital acquisitions to ensure compliance with the year 2000 (''Y2K'') problem would not be able to account for the full depreciation of these systems until 2005. Because HIPAA requires compliance before that time, the regulation would force premature obsolescence of this equipment because while it is Y2K compliant, it may be HIPAA non-compliant.

Response: This comment raises two distinct issues—(1) the investment in new equipment and (2) the compliance date. With regard to the first issue, we reject the comment's assertion that the regulation requires covered entities to purchase new information systems or information technology equipment, but realize that some covered entities may need to update their equipment. We have tried to minimize the costs, while responding appropriately to Congress' mandate for privacy rules. We have dealt with the cost issues in detail in the ''Regulatory Impact Analysis'' section of this Preamble. With regard to the second issue, Congress, not the Secretary, established the compliance data at section 1175(b) of the Act.

Civil Rights of Institutionalized Persons Act

Comment: A few comments expressed concern that the privacy regulation would inadvertently hinder the Department of Justice Civil Rights Divisions' investigations under the Civil Rights of Institutionalized Persons Act (''CRIPA''). These comments suggested clearly including civil rights enforcement activities as health care oversight.

Response: We agree with this comment. We do not intend for the privacy rules to hinder CRIPA investigations. Thus, the final rule includes agencies that are authorized by law to ''enforce civil rights laws for which health information is relevant'' in the definition of ''health oversight agency'' at § 164.501. Covered entities are permitted to disclose protected health information to health oversight agencies under § 164.512(d) without an authorization. Therefore, we do not believe the final rule should hinder the Department of Justice's ability to conduct investigations pursuant to its authority in CRIPA.

Clinical Laboratory Improvement Amendments

Comment: One comment expressed concern that the proposed definition of health care operations did not include activities related to the quality control clinical studies performed by laboratories to demonstrate the quality of patient test results. Because the Clinical Laboratory Improvement Amendments of 1988 (''CLIA'') requires these studies that the comment asserted require the use of protected health information, the comment suggested including this specific activity in the definition of ''health care operations.''

Response: We do not intend for the privacy regulation to impede the ability of laboratories to comply with the requirements of CLIA. Quality control activities come within the definition of ''health care operations'' in § 164.501 because they come within the meaning of the term ''quality assurance activities.'' To the extent they would not come within health care operations, but

are required by CLIA, the privacy regulation permits clinical laboratories that are regulated by CLIA to comply with mandatory uses and disclosures of protected health information pursuant to § 164.512(a).

Comment: One comment stated that the proposed regulation's right of access for inspection and copying provisions were contrary to CLIA in that CLIA permits laboratories to disclose lab test results only to ''authorized persons.'' This comment suggested that the final rule include language adopting this restriction to ensure that patients not obtain laboratory test results before the appropriate health care provider has reviewed and explained those results to the patients.

A similar comment stated that the lack of preemption of state laws could create problems for clinical laboratories under CLIA. Specifically, this comment noted that CLIA permits clinical laboratories to perform tests only upon the written or electronic request of, and to provide the results to, an ''authorized person.'' State laws define who is an ''authorized person.'' The comment expressed concern as to whether the regulation would preempt state laws that only permit physicians to receive test results.

Response: We agree that CLIA controls in these cases. Therefore, we have amended the right of access, § 164.524(a), so that a covered entity that is subject to CLIA does not have to provide access to the individual to the extent such access would be prohibited by law. Because of this change, we believe the preemption concern is moot.

Controlled Substance Act

Comment: One comment expressed concern that the privacy regulation as proposed would restrict the Drug Enforcement Agency's (''the DEA'') enforcement of the Controlled Substances Act (''CSA''). The comment suggested including enforcement activities in the definition of ''health oversight agency.''

Response: In our view, the privacy regulation should not impede the DEA's ability to enforce the CSA. First, to the extent the CSA requires disclosures to the DEA, these disclosures would be permissible under § 164.512(a). Second, some of the DEA's CSA activities come within the exception for health oversight agencies which permits disclosures to health oversight agencies for:

> Activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections * * * civil, administrative, or criminal proceedings or actions; and other activity necessary for appropriate oversight of the health care system.

Therefore, to the extent the DEA is enforcing the CSA, disclosures to it in its capacity as a health oversight agency are permissible under § 164.512(d). Alternatively, CSA required disclosures to the DEA for law enforcement purposes are permitted under § 164.512(f). When acting as a law enforcement agency under the CSA, the DEA may obtain the information pursuant to § 164.512(f). Thus, we do not agree that the privacy regulation will impede the DEA's enforcement of the CSA. See the preamble discussion of § 164.512 for further explanation.

Comment: One commenter suggested clarifying the provisions allowing disclosures that are ''required by law'' to ensure that the mandatory reporting requirements the CSA imposes on covered entities, including making available reports, inventories, and records of transactions, are not preempted by the regulation.

Response: We agree that the privacy regulation does not alter covered entities' obligations under the CSA. Because the CSA requires covered entities manufacturing, distributing, and/or dispensing controlled substances to maintain and provide to the DEA specific records and reports, the privacy regulation permits these disclosures under § 164.512(a). In addition, when the DEA seeks documents to determine an entity's compliance with the CSA, such disclosures are permitted under § 164.512(d).

Comment: The same commenter expressed concern that the proposed privacy regulation inappropriately limits voluntary reporting and would prevent or deter employees of covered entities from providing the DEA with information about violations of the CSA.

Response: We agree with the general concerns expressed in this comment. We do not believe the privacy rules will limit voluntary reporting of violations of the CSA. The CSA requires certain entities to maintain several types of records that may include protected health information. Although reports that included protected health information may be restricted under these rules, reporting the fact that an entity is not maintaining proper reports is not. If it were necessary to obtain protected health information during the investigatory stages following such a voluntary report, the DEA would be able to obtain the information in other ways, such as by following the administrative procedures outlined in § 164.512(e).

We also agree that employees of covered entities who report violations of the CSA should not be subjected to retaliation by their employers. Under § 164.502(j), we specifically state that a covered entity is not considered to have violated the regulation if a workforce member or business associate in good faith reports violations of laws or professional standards by covered entities to appropriate authorities. See discussion of § 164.502(j) below.

Department of Transportation

Comment: Several commenters stated that the Secretary should recognize in the preamble that it is permissible for employers to condition employment on an individual's delivering a consent to certain medical tests and/or examinations, such as drug-free workplace programs and Department of Transportation (''DOT'')-required physical examinations. These comments also suggested that employers should be able to receive certain information, such as pass/fail test and examination results, fitness-to-work assessments, and other legally required or permissible physical assessments without obtaining an authorization. To achieve this goal, these comments suggested defining ''health information'' to exclude information such as information about how much weight a specific employee can lift.

Response: We reject the suggestion to define ''health information,'' which Congress defined in HIPAA, so that it excludes individually identifiable health information that may be relevant to employers for these types of examinations and programs. We do not regulate employers. Nothing in the rules prohibit employers from conditioning employment on an individual signing the appropriate consent or authorization. By the same token, however, the rules below do not relieve employers from their obligations under the ADA and other laws that restrict the disclosure of individually identifiable health information.

Comment: One commenter asserted that the proposed regulation conflicts with the DOT guidelines regarding positive alcohol and drug tests that require the employer be notified in writing of the results. This document contains protected health information. In addition, the treatment center records must be provided to the Substance Abuse Professional (''SAP'') and the employer must receive a report from SAP with random drug testing recommendations.

Response: It is our understanding that DOT requires drug testing of all applicants for employment in safety-sensitive positions or individuals being transferred to such positions.

Employers, pursuant to DOT regulations, may condition an employee's employment or position upon first obtaining an authorization for the disclosure of results of these tests to the employer. Therefore, we do not believe the final rules conflict with the DOT requirements, which do not prohibit obtaining authorizations before such information is disclosed to employers.

Developmental Disabilities Act

Comment: One commenter urged HHS to ensure that the regulation would not impede access to individually identifiable health information to entities that are part of the Protection and Advocacy System to investigate abuse and neglect as authorized by the Developmental Disabilities Bill of Rights Act.

Response: The Developmental Disabilities Assistance and Bill of Rights Act of 2000 (''DD Act'') mandates specific disclosures of individually identifiable health information to Protection and Advocacy systems designated by the chief elected official of the states and Territories. Therefore, covered entities may make these disclosures under § 164.512(a) without first obtaining an individual's authorization, except in those circumstances in which the DD Act requires the individual's authorization. Therefore, the rules below will not impede the functioning of the existing Protection and Advocacy System.

Employee Retirement Income Security Act of 1974

Comment: Several commenters objected to the fact that the NPRM did not clarify the scope of preemption of state laws under the Employee Retirement Income Security Act of 1974 (ERISA). These commenters asserted that the final rule must state that ERISA preempts all state laws (including those relating to the privacy of individually identifiable health information) so that multistate employers could continue to administer their group health plans using a single set of rules. In contrast, other commenters criticized the Department for its analysis of the current principles governing ERISA preemption of state law, pointing out that the Department has no authority to interpret ERISA.

Response: This Department has no authority to issue regulations under ERISA as requested by some of these commenters, so the rule below does not contain the statement requested. See the discussion of this point under ''Preemption'' above.

Comment: One commenter requested that the final rule clarify that section 264(c)(2) of HIPAA does not save state laws that would otherwise be preempted by the Federal Employees Health Benefits Program. The commenter noted that in the NPRM this statement was made with respect to Medicare and ERISA, but not the law governing the FEHBP.

Response: We agree with this comment. The preemption analysis set out above with respect to ERISA applies equally to the Federal Employees Health Benefit Program.

Comment: One commenter noted that the final rule should clarify the interplay between state law, the preemption standards in Subtitle A of Title I of HIPAA (Health Care Access, Portability and Renewability), and the preemption standards in the privacy requirements in Subtitle F of Title II of HIPAA (Administrative Simplification).

Response: The NPRM described only the preemption standards that apply with respect to the statutory provisions of HIPAA that were implemented by the proposed rule. We agree that the preemption standards in Subtitle A of Title I of HIPAA are different. Congress expressly provided that the preemption provisions of Title I apply only to Part 7, which addresses portability, access, and renewability requirements for Group Health Plans. To the extent state laws contain provisions regarding portability, access, or renewability, as well as privacy requirements, a covered entity will need to evaluate the privacy provisions under the Title II preemption provisions, as explained in the preemption provisions of the rules, and the other provisions under the Title I preemption requirements.

European Union Privacy Directive and U.S. Safe Harbors

Comment: Several comments stated that the privacy regulation should be consistent with the European Union's Directive on Data Protection. Others sought guidance as to how to comply with both the E.U. Directive on Data Protection and the U.S. Safe Harbor Privacy Principles.

Response: We appreciate the need for covered entities obtaining personal data from the European Union to understand how the privacy regulation intersects with the Data Protection Directive. We have provided guidance as to this interaction in the ''Other Federal Laws'' provisions of the preamble.

Comment: A few comments expressed concern that the proposed definition of ''individual'' excluded foreign military and diplomatic personnel and their dependents, as well as overseas foreign national beneficiaries. They noted that the distinctions are based on nationality and are inconsistent with the stance of the E.U. Directive on Data Protection and the Department of Commerce's assurances to the European Commission.

Response: We agree with the general principle that privacy protections should protect every person, regardless of nationality. As noted in the discussion of the definition of ''individual,'' the final regulation's definition does not exclude foreign military and diplomatic personnel, their dependents, or overseas foreign national beneficiaries from the definition of individual. As described in the discussion of § 164.512 below, the final rule applies to foreign diplomatic personnel and their dependents like all other individuals. Foreign military personnel receive the same treatment under the final rule as U.S. military personnel do, as discussed with regard to § 164.512 below. Overseas foreign national beneficiaries to the extent they receive care for the Department of Defense or a source acting on behalf of the Department of Defense remain generally excluded from the final rules protections. For a more detailed explanation, see § 164.500.

Fair Credit Reporting Act

Comment: A few commenters requested that we exclude information maintained, used, or disclosed pursuant to the Fair Credit Reporting Act (''FCRA'') from the requirements of the privacy regulation. These commenters noted that the protection in the privacy regulation duplicate those in the FCRA.

Response: Although we realize that some overlap between FCRA and the privacy rules may exist, we have chosen not to remove information that may come within the purview of FCRA from the scope of our rules because FCRA's focus is not the same as our Congressional mandate to protect individually identifiable health information.

To the extent a covered entity seeks to engage in collection activities or other payment-related activities, it may do so pursuant to the requirements of this rule related to payment. See discussion of §§ 164.501 and 164.502 below.

We understand that some covered entities may be part of, or contain components that are, entities which meet the definition of ''consumer reporting agencies.'' As such, these entities are subject to the FCRA. As described in the preamble to § 164.504, covered entities must designate what parts of their organizations will be treated as covered entities for the

purpose of these privacy rules. The covered entity component will need to comply with these rules, while the components that are consumer reporting agencies will need to comply with FCRA.

Comment: One comment suggested that the privacy regulation would conflict with the FCRA if the regulation's requirement applied to information disclosed to consumer reporting agencies.

Response: To the extent a covered entity is required to disclose protected health information to a consumer reporting agency, it may do so under § 164.512(a). See also discussion under the definition of ''payment'' below.

Fair Debt Collection and Practices Act

Comment: Several comments expressed concern that health plans and health care providers be able to continue using debt collectors in compliance with the Fair Debt Collections Practices Act and related laws.

Response: In our view, health plans and health care providers will be able to continue using debt collectors. Using the services of a debt collector to obtain payment for the provision of health care comes within the definition of ''payment'' and is permitted under the regulation. Thus, so long as the use of debt collectors is consistent with the regulatory requirements (such as, providers obtain the proper consents, the disclosure is of the minimum amount of information necessary to collect the debt, the provider or health plan enter into a business associate agreement with the debt collector, etc.), relying upon debt collectors to obtain reimbursement for the provision of health care would not be prohibited by the regulation.

Family Medical Leave Act

Comment: One comment suggested that the proposed regulation adversely affects the ability of an employer to determine an employee's entitlement to leave under the Family Medical Leave Act (''FMLA'') by affecting the employer's right to receive medical certification of the need for leave, additional certifications, and fitness for duty certification at the end of the leave. The commenter sought clarification as to whether a provider could disclose information to an employer without first obtaining an individual's consent or authorization. Another commenter suggested that the final rule explicitly exclude from the rule disclosures authorized by the FMLA, because, in the commenter's view, it provides more than adequate protection for the confidentiality of medical records in the employment context.

Response: We disagree that the FMLA provides adequate privacy protections for individually identifiable health information. As we understand the FMLA, the need for employers to obtain protected health information under the statute is analogous to the employer's need for protected health information under the ADA. In both situations, employers may need protected health information to fulfill their obligations under these statutes, but neither statute requires covered entities to provide the information directly to the employer. Thus, covered entities in these circumstances will need an individual's authorizations before the disclosure is made to the employer.

Federal Common Law

Comment: One commenter did not want the privacy rules to interfere with the federal common law governing collective bargaining agreements permitting employers to insist on the cooperation of employees with medical fitness evaluations.

Response: We do not seek to interfere with legal medical fitness evaluations. These rules require a covered entity to have an individual's authorization before the information resulting from such evaluations is disclosed to the employer unless another provision of the rule applies. We do not prohibit employers from conditioning employment, accommodations, or other benefits, when legally permitted to do so, upon the individual/employee providing an authorization that would permit the disclosure of protected health information to employers by covered entities. See § 164.508(b)(4) below.

Federal Educational Rights and Privacy Act

Comment: A few commenters supported the exclusion of ''education records'' from the definition of ''protected health information.'' However, one commenter requested that ''treatment records'' of students who are 18 years or older attending post-secondary education institutions be excluded from the definition of ''protected health information'' as well to avoid confusion.

Response: We agree with these commenters. See ''Relationship to Other Federal Laws'' for a description of our exclusion of FERPA ''education records'' and records defined at 20 U.S.C. 1232g(a)(4)(B)(iv), commonly referred to as ''treatment records,'' from the definition of ''protected health information.''

Comment: One comment suggested that the regulation should not apply to any health information that is part of an ''education record'' in any educational agency or institution, regardless of its FERPA status.

Response: We disagree. As noted in our discussion of ''Relationship of Other Federal Laws,'' we exclude education records from the definition of protected health information because Congress expressly provided privacy protections for these records and explained how these records should be treated in FERPA.

Comment: One commenter suggested eliminating the preamble language that describes school nurses and on-site clinics as acting as providers and subject to the privacy regulation, noting that this language is confusing and inconsistent with the statements provided in the preamble explicitly stating that HIPAA does not preempt FERPA.

Response: We agree that this language may have been confusing. We have provided a clearer expression of when schools may be required to comply with the privacy regulation in the ''Relationship to Other Federal Laws'' section of the preamble.

Comment: One commenter suggested adding a discussion of FERPA to the ''Relationship to Other Federal Laws'' section of the preamble.

Response: We agree and have added FERPA to the list of federal laws discussed in ''Relationship to Other Federal Laws'' section of the preamble.

Comment: One commenter stated that school clinics should not have to comply with the ''ancillary'' administrative requirements, such as designating a privacy official, maintaining documentation of their policies and procedures, and providing the Secretary of HHS with access.

Response: We disagree. Because we have excluded education records and records described at 20 U.S.C. 1232g(a)(4)(B)(iv) held by educational agencies and institutions subject to FERPA from the definition of protected health information, only non-FERPA schools would be subject to the administrative requirements. Most of these school clinics will also not be covered entities because they are not engaged in HIPAA transactions and these administrative requirements will not apply to them. However, to the extent a school clinic is within the definition of a health care provider, as Congress defined the term, and the school clinic is engaged in HIPAA transactions, it will be a covered entity and must comply with the rules below.

Comment: Several commenters expressed concern that the privacy regulation would eliminate the parents' ability to have access to information in their children's school health records. Because the proposed regulation suggests that school-based clinics keep health records separate from other educational files, these comments argued that the regulation is contrary to the spirit of FERPA, which provides parents with access rights to their children's educational files.

Response: As noted in the ''Relationship to Other Federal Laws'' provision of the preamble, to the extent information in school-based clinics is not protected health information because it is an education record, the FERPA access requirements apply and this regulation does not. For more detail regarding the rule's application to unemancipated minors, see the preamble discussion about ''Personal Representatives.''

Federal Employees Compensation Act

Comment: One comment noted that the Federal Employees Compensation Act (''FECA'') requires claimants to sign a release form when they file a claim. This commenter suggested that the privacy regulation should not place additional restrictions on this type of release form.

Response: We agree. In the final rule, we have added a new provision, § 164.512(l), that permits covered entities to make disclosures authorized under workers' compensation and similar laws. This provision would permit covered entities to make disclosures authorized under FECA and not require a different release form.

Federal Employees Health Benefits Program

Comment: A few comments expressed concern about the preemption effect on FEHBP and wanted clarification that the privacy regulation does not alter the existing preemptive scope of the program.

Response: We do not intend to affect the preemptive scope of the FEHBP. The Federal Employee Health Benefit Act of 1998 preempts any state law that ''relates to'' health insurance or plans. 5 U.S.C. 8902(m). The final rule does not attempt to alter the preemptive scope Congress has provided to the FEHBP.

Comment: One comment suggested that in the context of FEHBP HHS should place the enforcement responsibilities of the privacy regulation with Office of Personnel Management, as the agency responsible for administering the program.

Response: We disagree. Congress placed enforcement with the Secretary. *See* section 1176 of the Act.

Federal Rules of Civil Procedure

Comment: A few comments suggested revising proposed § 164.510(d) so that it is consistent with the existing discovery procedure under the Federal Rules of Civil Procedure or local rules.

Response: We disagree that the rules regarding disclosures and uses of protected health information for judicial and administrative procedures should provide only those protections that exist under existing discovery rules. Although the current process may be appropriate for other documents and information requested during the discovery process, the current system, as exemplified by the Federal Rules of Civil Procedure, does not provide sufficient protection for protected health information. Under current discovery rules, private attorneys, government officials, and others who develop such requests make the initial determinations as to what information or documentation should be disclosed. Independent third-party review, such as that by a court, only becomes necessary if a person of whom the request is made refuses to provide the information. If this happens, the person seeking discovery must obtain a court order or move to compel discovery. In our view this system does not provide sufficient protections to ensure that unnecessary and unwarranted disclosures of protected health information does not occur. For a related discuss, see the preamble regarding ''Disclosures for Judicial and Administrative Proceedings'' under § 164.512(e).

Federal Rules of Evidence

Comment: Many comments requested clarification that the privacy regulation does not conflict or interfere with the federal or state privileges. In particular, one of these comments suggested that the final regulation provide that disclosures for a purpose recognized by the regulation not constitute a waiver of federal or state privileges.

Response: We do not intend for the privacy regulation to interfere with federal or state rules of evidence that create privileges. Consistent with The Uniform Health-Care Information Act drafted by the National Conference of Commissioners on Uniform State Laws, we do not view a consent or an authorization to function as a waiver of federal or state privileges. For further discussion of the effect of consent or authorization on federal or state privileges, see preamble discussions in §§ 164.506 and 164.508.

Comment: Other comments applauded the Secretary's references to *Jaffee* v. *Redman,* 518 U.S. 1 (1996), which recognized a psychotherapist-patient privilege, and asked the Secretary to incorporate expressly this privilege into the final regulation.

Response: We agree that the psychotherapist-patient relationship is an important one that deserves protection. However, it is beyond the scope our mandate to create specific evidentiary privileges. It is also unnecessary because the United States Supreme Court has adopted this privilege.

Comment: A few comments discussed whether one remedy for violating the privacy regulation should be to exclude or suppress evidence obtained in violation of the regulation. One comment supported using this penalty, while another opposed it.

Response: We do not have the authority to mandate that courts apply or not apply the exclusionary rule to evidence obtained in violation of the regulation. This issue is in the purview of the courts.

Federal Tort Claims Act

Comment: One comment contended that the proposed regulation's requirement mandating covered entities to name the subjects of protected health information disclosed under a business partner contract as third party intended beneficiaries under the contract would have created an impermissible right of action against the government under the Federal Tort Claims Act (''FTCA'').

Response: Because we have deleted the third party beneficiary provisions from the final rules, this comment is moot.

Comment: Another comment suggested the regulation would hamper the ability of federal agencies to disclose protected health information to their attorneys, the Department of Justice, during the initial stages of the claims brought under the FTCA.

Response: We disagree. The regulation applies only to federal agencies that are covered entities. To the extent an agency is not a covered entity, it is not subject to the regulation; to the extent an agency is a covered entity, it must comply with the regulation. A covered entity that is a federal agency may disclose relevant information to its attorneys, who are business associates, for purposes of health care operations, which includes uses or disclosures for legal functions. See § 164.501 (definitions of ''business associate'' and ''health care operations''). The final rule provides specific provisions describing how federal agencies may provide

adequate assurances for these types of disclosures of protected health information. See § 164.504(e)(3).

Food and Drug Administration

Comment: A few comments expressed concerns about the use of protected health information for reporting activities to the Food and Drug Administration (''FDA''). Their concern focused on the ability to obtain or disclose protected health information for pre-and post-marketing adverse event reports, device tracking, and post-marketing safety and efficacy evaluation.

Response: We agree with this comment and have provided that covered entities may disclose protected health information to persons subject to the jurisdiction of the FDA, to comply with the requirements of, or at the direction of, the FDA with regard to reporting adverse events (or similar reports with respect to dietary supplements), the tracking of medical devices, other post-marketing surveillance, or other similar requirements described at § 164.512(b).

Foreign Standards

Comment: One comment asked how the regulation could be enforced against foreign countries (or presumably entities in foreign countries) that solicit medical records from entities in the United States.

Response: We do not regulate solicitations of information. To the extent a covered entity wants to comply with a request for disclosure of protected health information to foreign countries or entities within foreign countries, it will need to comply with the privacy rules before making the disclosure. If the covered entity fails to comply with the rules, it will be subject to enforcement proceedings.

Freedom of Information Act

Comment: One comment asserted that the proposed privacy regulation conflicts with the Freedom of Information Act (''FOIA''). The comment argued that the proposed restriction on disclosures by agencies would not come within one of the permissible exemptions to the FOIA. In addition, the comment noted that only in exceptional circumstances would the protected health information of deceased individuals come within an exemption because, for the most part, death extinguishes an individual's right to privacy.

Response: Section 164.512(a) below permits covered entities to disclose protected health information when such disclosures are required by other laws as long as they follow the requirements of those laws. Therefore, the privacy regulation will not interfere with the ability of federal agencies to comply with FOIA, when it requires the disclosure.

We disagree, however, that most protected health information will not come within Exemption 6 of FOIA. See the discussion above under ''Relationship to Other Federal Laws'' for our review of FOIA. Moreover, we disagree with the comment's assertion that the protected health information of deceased individuals does not come within Exemption 6. Courts have recognized that a deceased individual's surviving relatives may have a privacy interest that federal agencies may consider when balancing privacy interests against the public interest in disclosure of the requested information. Federal agencies will need to consider not only the privacy interests of the subject of the protected health information in the record requested, but also, when appropriate, those of a deceased individual's family consistent with judicial rulings.

If an agency receives a FOIA request for the disclosure of protected health information of a deceased individual, it will need to determine whether or not the disclosure comes within Exemption 6. This evaluation must be consistent with the court's rulings in this area. If the exemption applies, the federal agency will not have to release the information. If the federal agency determines that the exemption does not apply, may release it under § 164.512(a) of this regulation.

Comment: One commenter expressed concern that our proposal to protect the individually identifiable health information about the deceased for two years following death would impede public interest reporting and would be at odds with many state Freedom of Information laws that make death records and autopsy reports public information. The commenter suggested permitting medical information to be available upon the death of an individual or, at the very least, that an appeals process be permitted so that health information trustees would be allowed to balance the interests in privacy and in public disclosure and release or not release the information accordingly.

Response: These rules permit covered entities to make disclosures that are required by state Freedom of Information Act (FOIA) laws under § 164.512(a). Thus, if a state FOIA law designates death records and autopsy reports as public information that must be disclosed, a covered entity may disclose it without an authorization under the rule. To the extent that such information is required to be disclosed by FOIA or other law, such disclosures are permitted under the final rule. In addition, to the extent that death records and autopsy reports are obtainable from non-covered entities, such as state legal authorities, access to this information is not impeded by this rule.

If another law does not require the disclosure of death records and autopsy reports generated and maintained by a covered entity, which are protected health information, covered entities are not allowed to disclose such information except as permitted or required by the final rule, even if another entity discloses them.

Comment: One comment sought clarification of the relationship between the Freedom of Information Act, the Privacy Act, and the privacy rules.

Response: We have provided this analysis in the ''Relationship to Other Federal Laws'' section of the preamble in our discussion of the Freedom of Information Act.

Gramm-Leach-Bliley

Comments: One commenter noted that the Financial Services Modernization Act, also known as Gramm-Leach-Bliley (''GLB''), requires financial institutions to provide detailed privacy notices to individuals. The commenter suggested that the privacy regulation should not require financial institutions to provide additional notice.

Response: We disagree. To the extent a covered entity is required to comply with the notice requirements of GLB and those of our rules, the covered entity must comply with both. We will work with the FTC and other agencies implementing GLB to avoid unnecessary duplication. For a more detailed discussion of GLB and the privacy rules, see the ''Relationship to Other Federal Laws'' section of the preamble.

Comment: A few commenters asked that the Department clarify that financial institutions, such as banks, that serve as payors are covered entities. The comments explained that with the enactment of the Gramm-Leach-Bliley Act, banks are able to form holding companies that will include insurance companies (that may be covered entities). They recommended that banks be held to the rule's requirements and be required to obtain authorization to conduct non-payment activities, such as for the marketing of health and non-health items and services or the use and disclosure to non-health related divisions of the covered entity.

Response: These comments did not provide specific facts that would permit us to provide a substantive response. An organization will need to determine whether it comes within the definition of ''covered entity.'' An organization may also need to consider whether or not it contains a health care component. Organizations that are uncertain about the application of the regulation to them will need to evaluate their specific facts in light of this rule.

Inspector General Act

Comment: One comment requested the Secretary to clarify in the preamble that the privacy regulation does not preempt the Inspector General Act.

Response: We agree that to the extent the Inspector General Act requires uses or disclosures of protected health information, the privacy regulation does not preempt it. The final rule provides that to the extent required under section 201(a)(5) of the Act, nothing in this subchapter should be construed to diminish the authority of any Inspector General, including the authority provided in the Inspector General Act of 1978. See discussion of § 160.102 above.

Medicare and Medicaid

Comment: One comment suggested possible inconsistencies between the regulation and Medicare/Medicaid requirements, such as those under the Quality Improvement System for Managed Care. This commenter asked that HHS expand the definition of health care operations to include health promotion activities and avoid potential conflicts.

Response: We disagree that the privacy regulation would prohibit managed care plans operating in the Medicare or Medicaid programs from fulfilling their statutory obligations. To the extent a covered entity is required by law to use or disclose protected health information in a particular manner, the covered entity may make such a use or disclosure under § 164.512(a). Additionally, quality assessment and improvement activities come within the definition of ''health care operations.'' Therefore, the specific example provided by the commenter would seem to be a permissible use or disclosure under § 164.502, even if it were not a use or disclosure ''required by law.''

Comment: One commenter stated that Medicare should not be able to require the disclosure of psychotherapy notes because it would destroy a practitioner's ability to treat patients effectively.

Response: If the Title XVIII of the Social Security Act requires the disclosure of psychotherapy notes, the final rule permits, but does not require, a covered entity to make such a disclosure under § 164.512(a). If, however, the Social Security Act does not require such disclosures, Medicare does not have the discretion to require the disclosure of psychotherapy notes as a public policy matter because the final rule provides that covered entities, with limited exceptions, must obtain an individual's authorization before disclosing psychotherapy notes. See § 164.508(a)(2).

National Labor Relations Act

Comment: A few comments expressed concern that the regulation did not address the obligation of covered entities to disclose protected health information to collective bargaining representatives under the National Labor Relations Act.

Response: The final rule does not prohibit disclosures that covered entities must make pursuant to other laws. To the extent a covered entity is required by law to disclose protected health information to collective bargaining representatives under the NLRA, it may to so without an authorization. Also, the definition of ''health care operations'' at § 164.501 permits disclosures to employee representatives for purposes of grievance resolution.

Organ Donation

Comment: One commenter expressed concern about the potential impact of the regulation on the organ donation program under 42 CFR part 482.

Response: In the final rule, we add provisions allowing the use or disclosure of protected health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating donation and transplantation. See § 164.512(h).

Privacy Act Comments

Comment: One comment suggested that the final rule unambiguously permit the continued operation of the statutorily established or authorized discretionary routine uses permitted under the Privacy Act for both law enforcement and health oversight.

Response: We disagree. See the discussion of the Privacy Act in ''Relationship to Other Federal Laws'' above.

Public Health Services Act

Comment: One comment suggested that the Public Health Service Act places more stringent rules regarding the disclosure of information on Federally Qualified Health Centers than the proposed privacy regulation suggested. Therefore, the commenter suggested that the final rule exempt Federally Qualified Health Centers from the rules requirements

Response: We disagree. Congress expressly included Federally Qualified Health Centers, a provider of medical or other health services under the Social Security Act section 1861(s), within its definition of health care provider in section 1171 of the Act; therefore, we cannot exclude them from the regulation.

Comment: One commenter noted that no conflicts existed between the proposed rule and the Public Health Services Act.

Response: As we discuss in the ''Relationship to Other Federal Laws'' section of the preamble, the Public Health Service Act contains explicit confidentiality requirements that are so general as not to create problems of inconsistency. We recognized, however, that in some cases, that law or its accompanying regulations may contain greater restrictions. In those situations, a covered entity's ability to make what are permissive disclosures under this privacy regulation would be limited by those laws.

Reporting Requirement

Comment: One comment noted that federal agencies must provide information to certain entities pursuant to various federal statutes. For example, federal agencies must not withhold information from a Congressional oversight committee or the General Accounting Office. Similarly, some federal agencies must provide the Bureau of the Census and the National Archives and Records Administration with certain information. This comment expressed concern that the privacy regulation would conflict with these requirements. Additionally, the commenter asked whether the privacy notice would need to contain these uses and disclosures and recommended that a general statement that these federal agencies would disclose protected health information when required by law be considered sufficient to meet the privacy notice requirements.

Response: To the extent a federal agency acting as a covered entity is required by federal statute to disclose protected health information, the regulation permits the disclosure as required by law under § 164.512(a). The notice provisions at § 164.520(b)(1)(ii)(B) require covered entities to provide a brief description of the purposes for which the covered

entity is permitted or required by the rules to use or disclose protected health information without an individual's written authorization. If these statutes require the disclosures, covered entities subject to the requirement may make the disclosure pursuant to § 164.512(a). Thus, their notice must include a description of the category of these disclosures. For example, a general statement such as the covered entity ''will disclose your protected health information to comply with legal requirements'' should suffice.

Comment: One comment stressed that the final rule should not inadvertently preempt mandatory reporting laws duly enacted by federal, state, or local legislative bodies. This commenter also suggested that the final rule not prevent the reporting of violations to law enforcement agencies.

Response: We agree. Like the proposed rule, the final rule permits covered entities to disclose protected health information when required by law under § 164.512(a). To the extent a covered entity is required by law to make a report to law enforcement agencies or is otherwise permitted to make a disclosure to a law enforcement agency as described in § 164.512(f), it may do so without an authorization. Alternatively, a covered entity may always request that individuals authorize these disclosures.

Security Standards

Comment: One comment called for HHS to consider the privacy regulation in conjunction with the other HIPAA standards. In particular, this comment focused on the belief that the security standards should be compatible with the existing and emerging health care and information technology industry standards.

Response: We agree that the security standards and the privacy rules should be compatible with one another and are working to ensure that the final rules in both areas function together. Because we are addressing comments regarding the privacy rules in this preamble, we will consider the comment about the security standard as we finalize that set of rules.

Substance Abuse Confidentiality Statute and Regulations

Comment: Several commenters noted that many health care providers are bound by the federal restrictions governing alcohol and drug abuse records. One commenter noted that the NPRM differed substantially from the substance abuse regulations and would have caused a host of practical problems for covered entities. Another commenter, however, supported the NPRM's analysis that stated that more stringent provisions of the substance abuse provisions would apply. This commenter suggested an even stronger approach of including in the text a provision that would preserve existing federal law. Yet, one comment suggested that the regulation as proposed would confuse providers by making it difficult to determine when they may disclose information to law enforcement because the privacy regulation would permit disclosures that the substance abuse regulations would not.

Response: We appreciate the need of some covered entities to evaluate the privacy rules in light of federal requirements regarding alcohol and drug abuse records. Therefore, we provide a more detailed analysis in the ''Relationship to Other Federal Laws'' section of the preamble.

Comment: Some of these commenters also noted that state laws contain strict confidentiality requirements. A few commenters suggested that HHS reassess the regulations to avoid inconsistencies with state privacy requirements, implying that problems exist because of conflicts between the federal and state laws regarding the confidentiality of substance abuse information.

Response: As noted in the preamble section discussing preemption, the final rules do not preempt state laws that provide more privacy protections. For a more detailed analysis of the relationship between state law and the privacy rules, see the ''Preemption'' provisions of the preamble.

Tribal Law

Comments: One commenter suggested that the consultation process with tribal governments described in the NPRM was inadequate under Executive Order No. 13084. In addition, the commenter expressed concern that the disclosures for research purposes as permitted by the NPRM would conflict with a number of tribal laws that offer individuals greater privacy rights with respect to research and reflects cultural appropriateness. In particular, the commenter referenced the Health Research Code for the Navajo Nation which creates a entity with broader authority over research conducted on the Navajo Nation than the local IRB and requires informed consent by study participants. Other laws mentioned by the commenter included the Navajo Nation Privacy and Access to Information Act and a similar policy applicable to all health care providers within the Navajo Nation. The commenter expressed concern that the proposed regulation research provisions would override these tribal laws.

Response: We disagree with the comment that the consultation with tribal governments undertaken prior to the proposed regulation is inadequate under Executive Order No. 13084. As stated in the proposed regulation, the Department consulted with representatives of the National Congress of American Indians and the National Indian Health Board, as well as others, about the proposals and the application of HIPAA to the Tribes, and the potential variations based on the relationship of each Tribe with the IHS for the purpose of providing health services. In addition, Indian and tribal governments had the opportunity to, and did, submit substantive comments on the proposed rules.

Additionally, disclosures permitted by this regulation do not conflict with the policies as described by this commenter. Disclosures for research purposes under the final rule, as in the proposed regulation, are permissive disclosures only. The rule describes the outer boundaries of permissible disclosures. A covered health care provider that is subject to the tribal laws of the Navajo Nation must continue to comply with those tribal laws. If the tribal laws impose more stringent privacy standards on disclosures for research, such as requiring informed consent in all cases, nothing in the final rule would preclude compliance with those more stringent privacy standards. The final rule does not interfere with the internal governance of the Navajo Nation or otherwise adversely affect the policy choices of the tribal government with respect to the cultural appropriateness of research conducted in the Navajo Nation.

TRICARE

Comment: One comment expressed concern regarding the application of the ''minimum necessary'' standard to investigations of health care providers under the TRICARE (formerly the CHAMPUS) program. The comment also expressed concern that health care providers would be able to avoid providing their records to such investigators because the proposed § 164.510 exceptions were not mandatory disclosures.

Response: In our view, neither the minimum necessary standard nor the final §§ 164.510 and 164.512 permissive disclosures will impede such investigations. The regulation requires covered entities to make all reasonable efforts not to disclose more than the minimum amount of protected health

information necessary to accomplish the intended purpose of the use or disclosure. This requirement, however, does not apply to uses or disclosures that are required by law. See § 164.502(b)(2)(iv). Thus, if the disclosure to the investigators is required by law, the minimum necessary standard will not apply. Additionally, the final rule provides that covered entities rely, if such reliance is reasonable, on assertions from public officials about what information is reasonably necessary for the purpose for which it is being sought. See § 164.514(d)(3)(iii).

We disagree with the assertion that providers will be able to avoid providing their records to investigators. Nothing in this rule permits covered entities to avoid disclosures required by other laws.

Veterans Affairs

Comment: One comment sought clarification about how disclosures of protected health information would occur within the Veterans Affairs programs for veterans and their dependents.

Response: We appreciate the commenter's request for clarification as to how the rules will affect disclosures of protected health information in the specific context of Veteran's Affairs programs. Veterans health care programs under 38 U.S.C. chapter 17 are defined as ''health plans.'' Without sufficient details as to the particular aspects of the Veterans Affairs programs that this comment views as problematic, we cannot comment substantively on this concern.

Comment: One comment suggested that the final regulation clarify that the analysis applied to the substance abuse regulations apply to laws governing Veteran's Affairs health records.

Response: Although we realize some difference may exist between the laws, we believe the discussion of federal substance abuse confidentiality regulations in the ''Relationship to Other Federal Laws'' preamble provides guidance that may be applied to the laws governing Veteran's Affairs (''VA'') health records. In most cases, a conflict will not exist between these privacy rules and the VA programs. For example, some disclosures allowed without patient consent or authorization under the privacy regulation may not be within the VA statutory list of permissible disclosures without a written consent. In such circumstances, the covered entity would have to abide by the VA statute, and no conflict exists. If the disclosures permitted by the VA statute come within the permissible disclosures of our rules, no conflict exists. In some cases, our rules may demand additional requirements, such as obtaining the approval of a privacy board or Institutional Review Board if a covered entity seeks to disclose protected health information for research purposes without the individual's authorization. A covered entity subject to the VA statute will need to ensure that it meets the requirements of both that statute and the regulation below. If a conflict arises, the covered entity should evaluate the specific potential conflicting provisions under the implied repeal analysis set forth in the ''Relationship to Other Federal Laws'' discussion in the preamble.

WIC

Comment: One comment called on other federal agencies to examine their regulations and policies regarding the use and disclosure of protected health information. The comment suggested that other agencies revise their regulations and policies to avoid duplicative, contradictory, or more stringent requirements. The comment noted that the U.S. Department of Agriculture's Special Supplemental Nutrition Program for Women, Infants, and Children (''WIC'') does not release WIC data. Because the commenter believed the regulation would not prohibit the disclosure of WIC data, the comment stated that the Department of Agriculture should now release such information.

Response: We support other federal agencies to whom the rules apply in their efforts to review existing regulations and policies regarding protected health information. However, we do not agree with the suggestion that other federal agencies that are not covered entities must reduce the protections or access-related rights they provide for individually identifiable health information they hold.

Part 160, Subpart C—Compliance and Enforcement

Section 160.306(a)—Who Can File Complaints With the Secretary

Comment: The proposed rule limited those who could file a complaint with the Secretary to individuals. A number of commenters suggested that other persons with knowledge of a possible violation should also be able to file complaints. Examples that were provided included a mental health care provider with first hand knowledge of a health plan improperly requiring disclosure of psychotherapy notes and an occupational health nurse with knowledge that her human resources manager is improperly reviewing medical records. A few comments raised the concern that permitting any person to file a complaint lends itself to abuse and is not necessary to ensure privacy rights and that the complainant should be a person for whom there is a duty to protect health information.

Response: As discussed below, the rule defines ''individual'' as the person who is the subject of the individually identifiable health information. However, the covered entity may allow other persons, such as personal representatives, to exercise the rights of the individual under certain circumstances, e.g., for a deceased individual. We agree with the commenters that any person may become aware of conduct by a covered entity that is in violation of the rule. Such persons could include the covered entity's employees, business associates, patients, or accrediting, health oversight, or advocacy agencies or organizations. Many persons, such as the covered entity's employees, may, in fact, be in a better position than the ''individual'' to know that a violation has occurred. Another example is a state Protection and Advocacy group that may represent persons with developmental disabilities. We have decided to allow complaints from any person. The term ''person'' is not restricted here to human beings or natural persons, but also includes any type of association, group, or organization.

Allowing such persons to file complaints may be the only way the Secretary may learn of certain possible violations. Moreover, individuals who are the subject of the information may not be willing to file a complaint because of fear of embarrassment or retaliation. Based on our experience with various civil rights laws, such as Title VI of the Civil Rights Act of 1964 and Title II of the Americans with Disabilities Act, that allow any person to file a complaint with the Secretary, we do not believe that this practice will result in abuse. Finally, upholding privacy protections benefits all persons who have or may be served by the covered entity as well as the general public, and not only the subject of the information.

If a complaint is received from someone who is not the subject of protected health information, the person who is the subject of this information may be concerned with the Secretary's investigation of this complaint. While we did not receive comments on this issue, we want to protect the privacy rights of this individual. This might

involve the Secretary seeking to contact the individual to provide information as to how the Secretary will address individual's privacy concerns while resolving the complaint. Contacting all individuals may not be practicable in the case of allegations of systemic violations (e.g., where the allegation is that hundreds of medical records were wrongfully disclosed).

Requiring That a Complainant Exhaust the Covered Entity's Internal Complaint Process Prior to Filing a Complaint With the Secretary

Comment: A number of commenters, primarily health plans, suggested that individuals should not be permitted to file a complaint with the Secretary until they exhaust the covered entity's own complaint process. Commenters stated that covered entities should have a certain period of time, such as ninety days, to correct the violation. Some commenters asserted that providing for filing a complaint with the Secretary will be very expensive for both the public and private sectors of the health care industry to implement. Other commenters suggested requiring the Secretary to inform the covered entity of any complaint it has received and not initiate an investigation or ''take enforcement action'' before the covered entity has time to address the complaint.

Response: We have decided, for a number of reasons, to retain the approach as presented in the proposed rule. First, we are concerned that requiring that complainants first notify the covered entity would have a chilling effect on complaints. In the course of investigating individual complaints, the Secretary will often need to reveal the identity of the complainant to the covered entity. However, in the investigation of cases of systemic violations and some individual violations, individual names may not need to be identified. Under the approach suggested by these commenters, the covered entity would learn the names of all persons who file complaints with the Secretary. Some individuals might feel uncomfortable or fear embarrassment or retaliation revealing their identity to the covered entity they believe has violated the regulation. Individuals may also feel they are being forced to enter into negotiations with this entity before they can file a complaint with the Secretary.

Second, because some potential complainants would not bring complaints to the covered entity, possible violations might not become known to the Secretary and might continue. Third, the delay in the complaint coming to the attention of the Secretary because of the time allowed for the covered entity to resolve the complaint may mean that significant violations are not addressed expeditiously. Finally, the process proposed by these commenters is arguably unnecessary because an individual who believes that an agreement can be reached with the covered entity, can, through the entity's internal complaint process or other means, seek resolution before filing a complaint with the Secretary.

Our approach is consistent with other laws and regulations protecting individual rights. None of the civil rights laws enforced by the Secretary require a complainant to provide any notification to the entity that is alleged to have engaged in discrimination (e.g., Americans with Disabilities Act, section 504 of the Rehabilitation Act, Title VI of the Civil Rights Act, and the Age Discrimination Act). The concept of ''exhaustion'' is used in laws that require individuals to pursue administrative remedies, such as that provided by a governmental agency, before bringing a court action. Under HIPAA, individuals do not have a right to court action.

Some commenters seemed to believe that the Secretary would pursue enforcement action without notifying the covered entity. It has been the Secretary's practice in investigating cases under other laws, such as various civil rights laws, to inform entities that we have received a complaint against them and to seek early resolution if possible. In enforcing the privacy rule, the Secretary will generally inform the covered entity of the nature of any complaints it has received against the entity. (There may be situations where information is withheld to protect the privacy interests of the complainant or others or where revealing information would impede the investigation of the covered entity.) The Secretary will also generally afford the entity an opportunity to share information with the Secretary that may result in an early resolution. Our approach will be to seek informal resolution of complaints whenever possible, which includes allowing covered entities a reasonable amount of time to work with the Secretary to come into compliance before initiating action to seek civil monetary penalties.

Section 160.306(b)(3)—Requiring That Complaints Be Filed With the Secretary Within a Certain Period of Time

Comment: A number of commenters, primarily privacy and disability advocacy organizations, suggested that the regulation require that complaints be filed with the Secretary by a certain time. These commenters generally recommended that the time period for filing a complaint should commence to run from the time when the individual knew or had reason to know of the violation or omission. Another comment suggested that a requirement to file a complaint with the Secretary within 180 days of the alleged noncompliance is a problem because a patient may, because of his or her medical condition, be unable to access his or her records within that time frame.

Response: We agree with the commenters that complainants should generally be required to submit complaints in a timely fashion. Federal regulations implementing Title VI of the Civil Rights Act of 1964 provide that ''[a] complaint must be filed not later than '180 days from the date of the alleged discrimination' unless the time for filing is extended by the responsible Department official or his designee.'' 45 CFR 80.7(b). Other civil rights laws, such as the Age Discrimination Act, section 504 of the Rehabilitation Act, and Title II of the Americans with Disabilities Act (ADA) (state and local government services), also use this approach. Under civil rights laws administered by the EEOC, individuals have 180 days of the alleged discriminatory act to file a charge with EEOC (or 300 days if there is a state or local fair employment practices agency involved).

Therefore, in the final rule we require that complaints be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred unless this time limit is waived by the Secretary for good cause shown. We believe that an investigation of a complaint is likely to be most effective if persons can be interviewed and documents reviewed as close to the time of the alleged violation as possible. Requiring that complaints generally be filed within a certain period of time increases the likelihood that the Secretary will have necessary and reliable information. Moreover, we are taking this approach in order to encourage complainants to file complaints as soon as possible. By receiving complaints in a timely fashion, we can, if such complaints prove valid, reduce the harm caused by the violation.

Section 160.308—Basis for Conducting Compliance Reviews

Comment: A number of comments expressed concern that the Secretary would conduct compliance reviews

without having received a complaint or having reason to believe there is noncompliance. A number of these commenters appeared to believe that the Secretary would engage in ''routine visits.'' Some commenters suggested that the Secretary should only be able to conduct compliance reviews if the Secretary has initiated an investigation of a complaint regarding the covered entity in the preceding twelve months. Some commenters suggested that there should only be compliance reviews based on established criteria for reviews (e.g., finding of ''reckless disregard''). Many of these commenters stated that cooperating with compliance reviews is potentially burdensome and expensive.

One commenter asked whether the Secretary will have a process for reviewing all covered entities to determine how they are complying with requirements. This commenter questioned whether covered entities will be required to submit plans and wait for Departmental approval.

Another commenter suggested that the Secretary specify a time limit for the completion of a compliance review.

Response: We disagree with the commenters that the final rule should restrict the Secretary's ability to conduct compliance reviews. The Secretary needs to maintain the flexibility to conduct whatever reviews are necessary to ensure compliance with the rule.

Section 160.310 (a) and (c)—The Secretary's Access to Information in Determining Compliance

Comment: Some commenters raised objections to provisions in the proposed rule which required that covered entities maintain records and submit compliance reports as the Secretary determines is necessary to determine compliance and required that covered entities permit access by the Secretary during normal business hours to its books, records, accounts, and other sources of information, including protected health information, and its facilities, that are pertinent to ascertaining compliance with this subpart. One commenter stated that the Secretary's access to private health information without appropriate patient consent is contrary to the intent of HIPAA. Another commenter expressed the view that, because covered entities face criminal penalties for violations, these provisions violate the Fifth Amendment protections against forced self incrimination. Other commenters stated that covered entities should be given the reason the Secretary needs to have access to its books and records. Another commenter stated that there should be a limit to the frequency or extent of intrusion by the federal government into the business practices of a covered entity and that these provisions violate the Fourth Amendment of the Constitution.

Finally, a coalition of church plans suggested that the Secretary provide church plans with additional procedural safeguards to reduce unnecessary intrusion into internal church operations. These suggested safeguards included permitting HHS to obtain records and other documents only if they are relevant and necessary to compliance and enforcement activities related to church plans, requiring a senior official to determine the appropriateness of compliance-related activities for church plans, and providing church plans with a self-correcting period similar to that Congress expressly provided in Title I of HIPAA under the tax code.

Response: The final rule retains the proposed language in these two provisions with one change. The rule adds a provision indicating that the Secretary's access to information held by the covered entity may be at any time and without notice where exigent circumstances exist, such as where time is of the essence because documents might be hidden or destroyed. Thus, covered entities will generally receive notice before the Secretary seeks to access the entity's books or records.

Other than the exigent circumstances language, the language in these two provisions is virtually the same as the language in this Department's regulation implementing Title VI of the Civil Rights Act of 1964. 45 CFR 80.6(b) and (c). The Title VI regulation is incorporated by reference in other Department regulations prohibiting discrimination of the basis of disability. 45 CFR 84.61. Similar provisions allowing this Department access to recipient information is found in the Secretary's regulation implementing the Age Discrimination Act. 45 CFR 91.34. These provisions have not proved to be burdensome to entities that are subject to these civil rights regulations (i.e., all recipients of Department funds).

We do not interpret Constitutional case law as supporting the view that a federal agency's review of information pursuant to statutory mandate violates the Fifth Amendment protections against forced self incrimination. Nor would such a review of this information raise Fourth Amendment problems. See discussion above regarding Constitutional comments and responses.

We appreciate the concern that the Secretary not involve herself unnecessarily into the internal operations of church plans. However, by providing health insurance or care to their employees, church plans are engaging in a secular activity. Under the regulation, church plans are subject to the same compliance and enforcement requirements with which other covered entities must comply. Because Congress did not carve out specific exceptions or require stricter standards for investigations related to church plans, incorporating such measures into the regulation would be inappropriate.

Additionally, there is no indication that the regulation will directly interfere with the religious practices of church plans. Also, the regulation as written appropriately limits the ability of investigators to obtain information from covered entities. The regulation provides that the Secretary may obtain access only to information that is pertinent to ascertain compliance with the regulation. We do not anticipate asking for information that is not necessary to assess compliance with the regulation. The purpose of obtaining records and similar materials is to determine compliance, not to engage in any sort of review or evaluation of religious activities or beliefs. Therefore, we believe the regulation appropriately balances the need to access information to determine compliance with the desire of covered entities to avoid opening every record in their possession to the government.

Provision of Technical Assistance

Comment: A number of commenters inquired as to how a covered entity can request technical assistance from the Secretary to come into compliance. A number of commenters suggested that the Secretary provide interpretive guidance to assist with compliance. Others recommended that the Secretary have a contact person or privacy official, available by telephone or email, to provide guidance on the appropriateness of a disclosure or a denial of access. One commenter suggested that there be a formal process for a covered entity to submit compliance activities to the Secretary for prior approval and clarification. This commenter suggested that clarifications be published on a contemporaneous basis in the **Federal Register** to help correct any ambiguities and confusion in implementation. It was also suggested that the Secretary undertake an assessment of ''best practices'' of covered entities and document and promote the findings to serve as a convenient ''road map'' for other covered entities. Another commenter suggested that we work with providers to create implementation guidelines modeled after the interpretative

guidelines that HCFA creates for surveyors on the conditions of participation for Medicare and Medicaid contractors.

Response: While we have not in the final rule committed the Secretary to any specific model of providing guidance or assistance, we do state our intent, subject to budget and staffing constraints, to develop a technical assistance program that will include the provision of written material when appropriate to assist covered entities in achieving compliance. We will consider other models including HCFA's Medicare and Medicaid interpretative guidelines. Further information regarding the Secretary's technical assistance program may be provided in the **Federal Register** and on the HHS Office for Civil Rights (OCR) Web Site. While OCR plans to have fully trained staff available to respond to questions, its ability to provide individualized advice in regard to such matters as the appropriateness of a particular disclosure or the sufficiency of compliance activities will be based on staff resources and demands. The idea of looking at ''best practices'' and sharing information with all covered entities is a good one and we will explore how best to do this. We note that a covered entity is not excused from compliance with the regulation because of any failure to receive technical assistance or guidance.

Basis for Violation Findings and Enforcement

Comment: A number of commenters asked that covered entities not be liable for violations of the rule if they have acted in good faith. One commenter indicated that enforcement actions should not be pursued against covered entities that make legitimate business decisions about how to comply with the privacy standards.

Response: The commenters seemed to argue that even if a covered entity does not comply with a requirement of the rule, the covered entity should not be liable if there was an honest and sincere intention or attempt to fulfill its obligations. The final rule, however, does not take this approach but instead draws careful distinctions between what a covered entity must do unconditionally, and what a covered entity must make certain reasonable efforts to do. In addition, the final rule is clear as to the specific provisions where ''good faith'' is a consideration. For example, a covered entity is permitted to use and disclose protected health information without authorization based on criteria that includes a good faith belief that such use or disclosure is necessary to avert an imminent threat to health or safety (§ 164.512(j)(1)(i)). Therefore, covered entities need to pay careful attention to the specific language in each requirement. However, we note that many of these provisions can be implemented in a variety of ways; e.g, covered entities can exercise business judgement regarding how to conduct staff training.

As to enforcement, a covered entity will not necessarily suffer a penalty solely because an act or omission violates the rule. As we discuss elsewhere, the Department will exercise discretion to consider not only the harm done, but the willingness of the covered entity to achieve voluntary compliance. Further, the Administrative Simplification provisions of HIPAA provide that whether a violation was known or not is relevant in determining whether civil or criminal penalties apply. In addition, if a civil penalty applies, HIPAA allows the Secretary, where the failure to comply was due to reasonable cause and not to willful neglect, to delay the imposition of the penalty to allow the covered entity to comply. The Department will develop and release for public comment an enforcement regulation applicable to all the administrative simplification regulations that will address these issues.

Comment: One commenter asked whether hospitals will be vicariously liable for the violations of their employees and expressed concern that hospitals and other providers will be the ones paying large fines.

Response: The enforcement regulation will address this issue. However, we note that section 1128A(1) of the Social Security Act, which applies to the imposition of civil monetary penalties under HIPAA, provides that a principal is liable for penalties for the actions of its agent acting within the scope of the agency. Therefore, a covered entity will generally be responsible for the actions of its employees such as where the employee discloses protected health information in violation of the regulation.

Comment: A commenter expressed the concern that if a covered entity acquires a non-compliant health plan, it would be liable for financial penalties. This commenter suggested that, at a minimum, the covered entity be given a grace period of at least a year, but not less than six months to bring any acquisition up to standard. The commenter stated that the Secretary should encourage, not discourage, compliant companies to acquire non-compliant ones. Another commenter expressed a general concern about resolution of enforcement if an entity faced with a HIPAA complaint acquires or merges with an entity not covered by HIPAA.

Response: As discussed above, the Secretary will encourage voluntary efforts to cure violations of the rule, and will consider that fact in determining whether to bring a compliance action. We do not agree, however, that we should limit our authority to pursue violations of the rule if the situation warrants it.

Comment: One commenter was concerned about the ''undue risk'' of liability on originators of information, stemming from the fact that ''the number of covered entities is limited and they are unable to restrict how a recipient of information may use or re-disclose information * * *''

Response: Under this rule, we do not hold covered entities responsible for the actions of recipients of protected health information, unless the recipient is a business associate of the covered entity. We agree that it is not fair to hold covered entities responsible for the actions of persons with whom they have no on-going relationship, but believe it is fair to expect covered entities to hold their business associates to appropriate standards of behavior with respect to health information.

Other Compliance and Enforcement Comments

Comment: A number of comments raised questions regarding the Secretary's priorities for enforcement. A few commenters stated that they supported deferring enforcement until there is experience using the proposed standards. One organization asked that we clarify that the regulation does not replace or otherwise modify the self-regulatory/consumer empowerment approach to consumer privacy in the online environment.

Response: We have not made any decisions regarding enforcement priorities. It appears that some commenters believe that no enforcement action will be taken against a given covered entity until that entity has had some time to comply. Covered entities have two years to come into compliance with the regulation (three years in the case of small health plans). Some covered entities will have had experience using the standards prior to the compliance date. We do not agree that we should defer enforcement where violations of the rule occur. It would be wrong for covered entities to believe that enforcement action is based on their not having much experience in

using a particular standard or meeting another requirement.

We support a self-regulation approach in that we recognize that most compliance will be achieved by the voluntary activities of covered entities rather than by our enforcement activities. Our emphasis will be on education, technical assistance, and voluntary compliance and not on finding violations and imposing penalties. We also support a consumer empowerment approach. A knowledgeable consumer is key to the effectiveness of this rule. A consumer familiar with the requirements of this rule will be equipped to make choices regarding which covered entity will best serve their privacy interests and will know their rights under the rule and how they can seek redress for violations of this rule. Privacy-minded consumers will seek to protect the privacy rights of others by bringing concerns to the attention of covered entities, the public, and the Secretary. However, we do not agree that we should defer enforcement where violations of the rule occur.

Comment: One commenter expressed concern that by filing a complaint an individual would be required to reveal sensitive information to the public. Another commenter suggested that complaints regarding noncompliance in regard to psychotherapy notes should be made to a panel of mental health professionals designated by the Secretary. This commenter also proposed that all patient information be maintained as privileged, not be revealed to the public, and be kept under seal after the case is reviewed and closed.

Response: We appreciate this concern and will seek to ensure that individually identifiable health information and other personal information contained in complaints will not be available to the public. The privacy regulation provides, at § 160.310(c)(3), that protected health information obtained by the Secretary in connection with an investigation or compliance review will not be disclosed except if necessary for ascertaining or enforcing compliance with the regulation or if required by law. In addition, this Department generally seeks to protect the privacy of individuals to the fullest extent possible, while permitting the exchange of records required to fulfill its administrative and program responsibilities. The Freedom of Information Act, 5 U.S.C. 552, and the HHS implementing regulation, 45 CFR part 5, provide substantial protection for records about individuals where disclosure would constitute an unwarranted invasion of their personal privacy. In implementing the privacy regulation, OCR plans to continue its current practice of protecting its complaint files from disclosure. OCR treats these files as investigatory records compiled for law enforcement purposes. Moreover, OCR maintains that disclosing protected health information in these files generally constitutes an unwarranted invasion of personal privacy.

It is not clear in regarding the use of mental health professionals, whether the commenter believes that such professionals should be involved because they would be best able to keep psychotherapy notes confidential or because such professionals can best understand the meaning or relevance of such notes. OCR anticipates that it will not have to obtain a copy or review psychotherapy notes in investigating most complaints regarding noncompliance in regard to such notes. There may be some cases where a review of the notes may be needed such as where we need to identify that the information a covered entity disclosed was in fact psychotherapy notes. If we need to obtain a copy of psychotherapy notes, we will keep these notes confidential and secure. OCR investigative staff will be trained to ensure that they fully respect the confidentiality of personal information. In addition, while the specific contents of these notes is generally not relevant to violations under this rule, if such notes are relevant, we will secure the expertise of mental health professionals if needed in reviewing psychotherapy notes.

Comment: A member of Congress and a number of privacy and consumer groups expressed concern with whether OCR has adequate funding to carry out the major responsibility of enforcing the complaint process established by this rule. The Senator stated that ''[d]ue to the limited enforcement ability allowed for in this rule by HIPAA, it is essential that OCR have the capacity to enforce the regulations. Now is the time for OCR to begin building the necessary infrastructure to enforce the regulation effectively.''

Response: We agree and are committed to an effective enforcement program. We are working with Congress to ensure that the Secretary has the necessary funds to secure voluntary compliance through education and technical assistance, to investigate complaints and conduct compliance reviews, to provide states with exception determinations, and to use civil and criminal penalties when necessary. We will continue to work with Congress and within the new Administration in this regard.

Coordination With Reviewing Authorities

Comment: A number of commenters referenced other entities that already consider the privacy of health information. One commenter indicated opposition to the delegation of inspections to third party organizations, such as the Joint Commission on the Accreditation of Healthcare Organizations (JCAHO). A few commenters indicated that state agencies are already authorized to investigate violations of state privacy standards and that we should rely on those agencies to investigate alleged violations of the privacy rules or delegate its complaint process to states that wish to carry out this responsibility or to those states that have a complaint process in place. Another commenter argued that individuals should be required to exhaust any state processes before filing a complaint with the Secretary. Others referenced the fact that state medical licensing boards investigate complaints against physicians for violating patient confidentiality. One group asked that the federal government streamline all of these activities so physicians can have a single entity to whom they must be responsive. Another group suggested that OMB should be given responsibility for ensuring that FEHB Plans operate in compliance with the privacy standards and for enforcement.

A few commenters stated that the regulation might be used as a basis for violation findings and subsequent penalties under other Department authorities, such as under Medicare's Conditions of Participation related to patient privacy and right to confidentiality of medical records. One commenter wanted some assurance that this regulation will not be used as grounds for sanctions under Medicare. Another commenter indicated support for making compliance with the privacy regulation a Condition of Participation under Medicare.

Response: HIPAA does not give the Secretary the authority to delegate her responsibilities to other private or public agencies such as JCAHO or state agencies. However, we plan to explore ways that we may benefit from current activities that also serve to protect the privacy of individually identifiable health information. For example, if we conduct an investigation or review of a covered entity, that entity may want to share information regarding findings of other bodies that conducted similar reviews. We would welcome such

information. In developing its enforcement program, we may explore ways it can coordinate with other regulatory or oversight bodies so that we can efficiently and effectively pursue our joint interests in protecting privacy.

We do not accept the suggestion that individuals be required to exhaust their remedies under state law before filing a complaint with the Secretary. Our rationale is similar to that discussed above in regard to the suggestion that covered entities be required to exhaust a covered entity's internal complaint process before filing a complaint with the Secretary. Congress provided for federal privacy protection and we want to allow individuals the right to this protection without barriers or delay. Covered entities may in their privacy notice inform individuals of any rights they have under state law including any right to file privacy complaints. We do not have the authority to interfere with state processes and HIPAA explicitly provides that we cannot preempt state laws that provide greater privacy protection.

We have not yet addressed the issue as to whether this regulation might be used as a basis for violation findings or penalties under other Department authorities. We note that Medicare conditions of participation require participating providers to have procedures for ensuring the confidentiality of patient records, as well as afford patients with the right to the confidentiality of their clinical records.

Penalties

Comment: Many commenters considered the statutory penalties insufficient to protect privacy, stating that the civil penalties are too weak to have the impact needed to reduce the risk of inappropriate disclosure. Some commenters took the opposing view and stated that large fines and prison sentences for violations would discourage physicians from transmitting any sort of health care information to any other agency, regardless of the medical necessity. Another comment expressed the concern that doctors will be at risk of going to jail for protecting the privacy of individuals (by not disclosing information the government believes should be released).

Response: The enforcement regulation will address the application of the civil monetary and criminal penalties under HIPAA. The regulation will be published in the **Federal Register** as a proposed regulation and the public will have an opportunity to comment. We do not believe that our rule, and the penalties available under it, will discourage physicians and other providers from using or disclosing necessary information. We believe that the rule permits physicians to make the disclosures that they need to make under the health care system without exposing themselves to jeopardy under the rule. We believe that the penalties under the statute are woefully inadequate. We support legislation that would increase the amount of these penalties.

Comment: A number of commenters stated that the regulations should permit individuals to sue for damages caused by breaches of privacy under these regulations. Some of these commenters specified that damages, equitable relief, attorneys fees, and punitive damages should be available. Conversely, one comment stated that strong penalties are necessary and would preclude the need for a private right of action. Another commenter stated that he does not believe that the statute intended to give individuals the equivalent of a right to sue, which results from making individuals third party beneficiaries to contracts between business partners.

Response: We do not have the authority to provide a private right of action by regulation. As discussed below, the final rule deletes the third party beneficiary provision that was in the proposed rule.

However, we believe that, in addition to strong civil monetary penalties, federal law should allow any individual whose rights have been violated to bring an action for actual damages and equitable relief. The Secretary's Recommendations, which were submitted to Congress on September 11, 1997, called for a private right of action to permit individuals to enforce their privacy rights.

Comment: One comment stated that, in calculating civil monetary penalties, the criteria should include aggravating or mitigating circumstances and whether the violation is a minor or first time violation. Several comments stated that penalties should be tiered so that those that commit the most egregious violations face stricter civil monetary penalties.

Response: As mentioned above, issues regarding civil fines and criminal penalties will be addressed in the enforcement regulation.

Comment: One comment stated that the regulation should clarify whether a single disclosure that involved the health information of multiple parties would constitute a single or multiple infractions, for the purpose of calculating the penalty amount.

Response: The enforcement regulation will address the calculation of penalties. However, we note that section 1176 subjects persons to civil monetary penalties of not more than $100 for each violation of a requirement or prohibition and not more than $25,000 in a calendar year for all violations of an identical requirement or prohibition. For example, if a covered entity fails to permit amendment of protected health information for 10 patients in one calendar year, the entity may be fined up to $1000 ($100 times 10 violations equals $1000).

Part 164—Subpart A—General Requirements

Part 164—Subpart B–D—Reserved

Part 164—Subpart E—Privacy

Section 164.500—Applicability

Covered Entities

The response to comments on covered entities is included in the response to comments on the definition of ''covered entity'' in the preamble discussion of § 160.103.

Covered Information

The response to comments on covered information is included in the response to comments on the definition of ''protected health information'' in the preamble discussion of § 164.501.

Section 164.501—Definitions

Designated record set

Comment: Many commenters generally supported our proposed definition of designated record set. Commenters suggested different methods for narrowing the information accessible to individuals, such as excluding information obtained without face-to-face interaction (e.g., phone consultations). Other commenters recommended broadening the information accessible to individuals, such as allowing access to ''the entire medical record,'' not just a designated record set. Some commenters advocated for access to all information about individuals. A few commenters generally supported the provision but recommended that consultation and interpretative assistance be provided when the disclosure may cause harm or misunderstanding.

Response: We believe individuals should have a right to access any protected health information that may be used to make decisions about them and modify the final rule to accomplish this result. This approach facilitates an open and cooperative relationship between individuals and covered health care providers and health plans and allows individuals fair opportunities to know what health information may be

used to make decisions about them. We list certain records that are always part of the designated record set. For covered providers these are the medical record and billing record. For health plans these are the enrollment, payment, claims adjudication, and case or medical management records. The purpose of these specified records is management of the accounts and health care of individuals. In addition, we include in the designated record set to which individuals have access any record used, in whole or in part, by or for the covered entity to make decisions about individuals. Only protected health information that is in a designated record set is covered. Therefore, if a covered provider has a phone conversation, information obtained during that conversation is subject to access only to the extent that it is recorded in the designated record set.

We do not require a covered entity to provide access to all individually identifiable health information, because the benefits of access to information not used to make decisions about individuals is limited and is outweighed by the burdens on covered entities of locating, retrieving, and providing access to such information. Such information may be found in many types of records that include significant information not relevant to the individual as well as information about other persons. For example, a hospital's peer review files that include protected health information about many patients but are used only to improve patient care at the hospital, and not to make decisions about individuals, are not part of that hospital's designated record sets.

We encourage but do not require covered entities to provide interpretive assistance to individuals accessing their information, because such a requirement could impose administrative burdens that outweigh the benefits likely to accrue.

The importance to individuals of having the right to inspect and copy information about them is supported by a variety of industry groups and is recognized in current state and federal law. The July 1977 Report of the Privacy Protection Study Commission recommended that individuals have access to medical records and medical record information.[2] The Privacy Act (5 U.S.C. 552a) requires government agencies to permit individuals to review records and have a copy made in a form comprehensible to the individual. In its report ''Best Principles for Health Privacy,'' the Health Privacy Working Group recommended that individuals should have the right to access information about them.[3] The National Association of Insurance Commissioners' Health Information Privacy Model Act establishes the right of an individual to examine or receive a copy of protected health information in the possession of the carrier or a person acting on behalf of the carrier.

Many states also establish a right for individuals to access health information about them. For example, Alaska law (AK Code 18.23.005) entitles patients ''to inspect and copy any records developed or maintained by a health care provider or other person pertaining to the health care rendered to the patient.'' Hawaii law (HRS section 323C–11) requires health care providers and health plans, among others, to permit individuals to inspect and copy protected health information about them. Many other states have similar provisions.

Industry and standard-setting organizations also have developed policies to enable individual access to health information. The National Committee for Quality Assurance and the Joint Commission on Accreditation of Healthcare Organizations issued recommendations stating, ''Patients' confidence in the protection of their information requires that they have the means to know what is contained in their records. The opportunity for patients to review their records will enable them to correct any errors and may provide them with a better understanding of their health status and treatment.'' [4] Standards of the American Society for Testing and Materials state, ''The patient or his or her designated personal representative has access rights to the data and information in his or her health record and other health information databases except as restricted by law. An individual should be able to inspect or see his or her health information or request a copy of all or part of the health information, or both.'' [5] We build on this well-established principle in this final rule.

Comment: Several commenters advocated for access to not only information that has already been used to make decisions, but also information that may be used to make decisions. Other commenters believed accessible information should be more limited; for example, some commenters argued that accessible information should be restricted to only information used to make health care decisions.

Response: We agree that it is desirable that individuals have access to information reasonably likely to be used to make decisions about them. On the other hand, it is desirable that the category of records covered be readily ascertainable by the covered entity. We therefore define ''designated record set'' to include certain categories of records (a provider's medical record and billing record, the enrollment records, and certain other records maintained by a health plan) that are normally used, and are reasonably likely to be used, to make decisions about individuals. We also add a category of other records that are, in fact, used, in whole or in part, to make decisions about individuals. This category includes records that are used to make decisions about any individuals, whether or not the records have been used to make a decision about the particular individual requesting access.

We disagree that accessible information should be restricted to information used to make health care decisions, because other decisions by covered entities can also affect individuals' interests. For example, covered entities make financial decisions about individuals, such as whether an individual's deductible has been met. Because such decisions can significantly affect individuals' interests, we believe they should have access to any protected health information included in such records.

Comment: Some commenters believed the rule should use the term ''retrievable'' instead of ''retrieved'' to describe information accessible to individuals. Other commenters suggested that the rule follow the Privacy Act's principle of allowing access only when entities retrieve records by individual identifiers. Some commenters requested clarification that covered entities are not required to maintain information by name or other patient identifier.

Response: We have modified the proposed definition of the designated record set to focus on how information is used, not how it is retrieved. Information may be retrieved or retrievable by name, but if it is never used to make decisions about any

[2] Privacy Protection Study Commission, ''Personal Privacy in an Information Society,'' July 1977, p. 298–299.

[3] Health Privacy Working Group, ''Best Principles for Health Privacy,'' Health Privacy Project, Institute for Health Care Research and Policy, Georgetown University, July 1999.

[4] National Committee on Quality Assurance and the Joint Commission on Accreditation of Healthcare Organizations, ''Protecting Personal Health Information: A Framework for Meeting the Challenges in a Managed Care Environment,'' 1998, p. 25.

[5] ASTM, ''Standard Guide for Confidentiality, Privacy, Access and Data Security, Principles for Health Information Including Computer-Based Patient Records,'' E 1869–97, § 11.1.1.

individuals, the burdens of requiring a covered entity to find it and to redact information about other individuals outweigh any benefits to the individual of having access to the information. When the information might be used to affect the individual's interests, however, that balance changes and the benefits outweigh the burdens. We confirm that this regulation does not require covered entities to maintain any particular record set by name or identifier.

Comment: A few commenters recommended denial of access for information relating to investigations of claims, fraud, and misrepresentations. Many commenters suggested that sensitive, proprietary, and legal documents that are ''typical state law privileges'' be excluded from the right to access. Specific suggestions for exclusion, either from the right of access or from the definition of designated record set, include quality assurance activities, information related to medical appeals, peer review and credentialing, attorney-client information, and compliance committee activities. Some commenters suggested excluding information already supplied to individuals on previous requests and information related to health care operations. However, some commenters felt that such information was already excluded from the definition of designated record set. Other commenters requested clarification that this provision will not prevent patients from getting information related to medical malpractice.

Response: We do not agree that records in these categories are never used to affect the interests of individuals. For example, while protected health information used for peer review and quality assurance activities typically would not be used to make decisions about individuals, and, thus, typically would not be part of a designated record set, we cannot say that this is true in all cases. We design this provision to be sufficiently flexible to work with the varying practices of covered entities.

The rule addresses several of these comments by excepting from the access provisions (§ 164.524) information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding. Similarly, nothing in this rule requires a covered entity to divulge information covered by physician-patient or similar privilege. Under the access provisions, a covered entity may redact information in a record about other persons or information obtained under a promise of confidentiality, prior to releasing the information to the individual. We clarify that nothing in this provision would prevent access to information needed to prosecute or defend a medical malpractice action; the rules of the relevant court determine such access.

We found no persuasive evidence to support excluding information already supplied to individuals on previous requests. The burdens of tracking requests and the information provided pursuant to requests outweigh the burdens of providing the access requested. A covered entity may, however, discuss the scope of the request for access with the individual to facilitate the timely provision of access. For example, if the individual agrees, the covered entity could supply only the information created or received since the date access was last granted.

Disclosure

Comment: A number of commenters asked that the definition of ''disclosure'' be modified so that it is clear that it does not include the release, transfer, provision of access to, or divulging in any other manner of protected health information to the individual who is the subject of that information. It was suggested that we revise the definition in this way to clarify that a health care provider may release protected health information to the subject of the information without first requiring that the patient complete an authorization form.

Response: We agree with the commenters' concern, but accomplish this result through a different provision in the regulation. In § 164.502 of this final rule, we specify that disclosures of protected health information to the individual are not subject to the limitations on disclosure of protected health information otherwise imposed by this rule.

Comment: A number of commenters stated that the regulation should not apply to disclosures occurring within or among different subsidiaries or components of the same entity. One commenter interpreted ''disclosure'' to mean outside the agency or, in the case of a state Department of Health, outside sister agencies and offices that directly assist the Secretary in performing Medicaid functions and are listed in the state plan as entitled to receive Medicaid data.

Response: We agree that there are circumstances under which related organizations may be treated as a single covered entity for purposes of protecting the privacy of health information, and modify the rule to accommodate such circumstances. In § 164.504 of the final rule, we specify the conditions under which affiliated companies may combine into a single covered entity and similarly describe which components of a larger organization must comply with the requirements of this rule. For example, transfers of information within the designated component or affiliated entity are uses while transfers of information outside the designated component or affiliated entity are disclosures. See the discussion of § 164.504 for further information and rationale. It is not clear from these comments whether the particular organizational arrangements described could constitute a single covered entity.

Comment: A commenter noted that the definition of ''disclosure'' should reflect that health plan correspondence containing protected health information, such as Explanation of Benefits (EOBs), is frequently sent to the policyholder. Therefore, it was suggested that the words ''provision of access to'' be deleted from the definition and that a ''disclosure'' be clarified to include the conveyance of protected health information to a third party.

Response: The definition is, on its face, broad enough to cover the transfers of information described and so is not changed. We agree that health plans must be able to send EOBs to policyholders. Sending EOB correspondence to a policyholder by a covered entity is a disclosure for purposes of this rule, but it is a disclosure for purposes of payment. Therefore, subject to the provisions of § 164.522(b) regarding Confidential Communications, it is permitted even if it discloses to the policyholder protected health information about another individual (see below).

Health care operations

Comment: Several commenters stated that the list of activities within the definition of health care operations was too broad and should be narrowed. They asserted that the definition should be limited to exclude activities that have little or no connection to the care of a particular patient or to only include emergency treatment situations or situations constituting a clear and present danger to oneself or others.

Response: We disagree. We believe that narrowing the definition in the manner requested will place serious burdens on covered entities and impair their ability to conduct legitimate business and management functions.

Comment: Many commenters, including physician groups, consumer groups, and privacy advocates, argued that we should limit the information that can be used for health care operations to de-identified data. They

argued that if an activity could be done with de-identified data, it should not be incorporated in the definition of health care operations.

Response: We disagree. We believe that many activities necessary for the business and administrative operations of health plans and health care providers are not possible with de-identified information or are possible only under unduly burdensome circumstances. For example, identified information may be used or disclosed during an audit of claims, for a plan to contact a provider about alternative treatments for specific patients, and in reviewing the competence of health care professionals. Further, not all covered entities have the same ability to de-identify protected health information. Covered entities with highly automated information systems will be able to use de-identified data for many purposes. Other covered entities maintain most of their records on paper, so a requirement to de-identify information would place too great a burden on the legitimate and routine business functions included in the definition of health care operations. Small business, which are most likely to have largely paper records, would find such a blanket requirement particularly burdensome.

Protected health information that is de-identified pursuant to § 164.514(a) is not subject to this rule. We hope this provides covered entities capable of de-identifying information with the incentive to do so.

Comment: Some commenters requested that we permit the use of demographic data (geographic, location, age, gender, and race) separate from all other data for health care operations. They argued that demographic data was needed to establish provider networks and monitor providers to ensure that the needs of ethnic and minority populations were being addressed.

Response: The use of demographic data for the stated purposes is within the definition of health care operations; a special rule is not necessary.

Comment: Some commenters pointed out that the definition of health care operations is similar to, and at times overlaps with, the definition of research. In addition, a number of commenters questioned whether or not research conducted by the covered entity or its business partner must only be applicable to and used within the covered entity to be considered health care operations. Others questioned whether such studies or research performed internal to a covered entity are ''health care operations'' even if generalizable results may be produced.

Response: We agree that some health care operations have many of the characteristics of research studies and in the NPRM asked for comments on how to make this distinction. While a clear answer was not suggested in any of the comments, the comments generally together with our fact finding lead to the provisions in the final rule. The distinction between health care operations and research rests on whether the primary purpose of the study is to produce ''generalizable knowledge.'' We have modified the definition of health care operations to include ''quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, *provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities.*'' If the primary purpose of the activity is to produce generalizable knowledge, the activity fits within this rule's definition of ''research'' and the covered entity must comply with §§ 164.508 or 164.512, including obtaining an authorization or the approval of an institutional review board or privacy board. If not and the activity otherwise meets the definition of health care operations, the activity is not research and may be conducted under the health care operations provisions of this rule.

In some instances, the primary purpose of the activity may change as preliminary results are analyzed. An activity that was initiated as an internal outcomes evaluation may produce information that the covered entity wants to generalize. If the purpose of a study changes and the covered entity does intend to generalize the results, the covered entity should document the change in status of the activity to establish that they did not violate the requirements of this rule. (See definition of ''research,'' below, for further information on the distinction between ''research'' and ''health care operations.'')

We note that the difficulty in determining when an activity is for the internal operations of an entity and when it is a research activity is a long-standing issue in the industry. The variation among commenters' views is one of many indications that, today, there is not consensus on how to draw this line. We do not resolve the larger issue here, but instead provide requirements specific to the information covered by this rule.

Comment: Several commenters asked that disease management and disability management activities be explicitly included in the definition of health care operations. Many health plans asserted that they would not be able to provide disease management, wellness, and health promotion activities if the activity were solely captured in the rule's definition of ''treatment.'' They also expressed concern that ''treatment'' usually applies to an individual, not to a population, as is the practice for disease management.

Response: We were unable to find generally accepted definitions of the terms ''disease management'' and ''disability management.'' Rather than rely on this label, we include many of the functions often included in discussions of disease management in this definition or in the definition of treatment, and modify both definitions to address the commenters' concerns. For example, we have revised the definition of health care operations to include population-based activities related to improving health or reducing health care costs. This topic is discussed further in the comment responses regarding the definition of ''treatment,'' below.

Comment: Several commenters urged that the definition of health care operations be illustrative and flexible, rather than structured in the form of a list as in the proposed rule. They believed it would be impossible to identify all the activities that constitute health care operations. Commenters representing health plans were concerned that the ''static'' nature of the definition would stifle innovation and could not reflect the new functions that health plans may develop in the future that benefit consumers, improve quality, and reduce costs. Other commenters, expressed support for the approach taken in the proposed rule, but felt the list was too broad.

Response: In the final rule, we revise the proposed definition of health care operations to broaden the list of activities included, but we do not agree with the comments asking for an illustrative definition rather than an inclusive list. Instead, we describe the activities that constitute health care operations in broad terms and categories, such as ''quality assessment'' and ''business planning and development.'' We believe the use of broadly stated categories will allow industry innovation, but without the privacy risks entailed in an illustrative approach.

Comment: Several commenters noted that utilization review and internal quality review should be included in the definition. They pointed out that both of these activities were discussed in the preamble to the proposed rule but were not incorporated into the regulation text.

Response: We agree and have modified the regulation text to incorporate quality assessment and improvement activities, including the development of clinical guidelines and protocol development.

Comment: Several commenters stated that the proposal did not provide sufficient guidance regarding compiling and analyzing information in anticipation of or for use in legal proceedings. In particular, they raised concerns about the lack of specificity as to when ''anticipation'' would be triggered.

Response: We agree that this provision was confusing and have replaced it with a broader reference to conducting or arranging for legal services generally.

Comment: Hospital representatives pointed out the pressure on health care facilities to improve cost efficiencies, make cost-effectiveness studies, and benchmark essential health care operations. They emphasized that such activities often use identifiable patient information, although the products of the analyses usually do not contain identifiable health information. Commenters representing state hospital associations pointed out that they routinely receive protected health information from hospitals for analyses that are used by member hospitals for such things as quality of care benchmark comparisons, market share analysis, determining physician utilization of hospital resources, and charge comparisons.

Response: We have expanded the definition of health care operations to include use and disclosure of protected health information for the important functions noted by these commenters. We also allow a covered entity to engage a business associate to provide data aggregation services. See § 164.504(e).

Comment: Several commenters argued that many activities that are integral to the day-to-day operations of a health plan have not been included in the definition. Examples provided by the commenters include: issuing plan identification cards, customer service, computer maintenance, storage and back-up of radiologic images, and the installation and servicing of medical equipment or computer systems.

Response: We agree with the commenters that there are activities not directly part of treatment or payment that are more closely associated with the administrative or clerical functions of the plan or provider that need to be included in the definition. To include such activities in the definition of health care operations, we eliminate the requirement that health care operations be directly related to treatment and payment, and we add to this definition the new categories of business management (including general administrative activities) and business planning activities.

Comment: One commenter asked for clarification on whether cost-related analyses could also be done by providers as well as health plans.

Response: Health care operations, including business management functions, are not limited to health plans. Any covered entity can perform health care operations.

Comment: One commenter stated that the proposed rule did not address what happens to records when a covered entity is sold or merged with another entity.

Response: We agree and add to the definition of health care operations disclosures of protected health information for due diligence to a covered entity that is a potential successor in interest. This provision includes disclosures pursuant to the sale of a covered entity's business as a going concern, mergers, acquisitions, consolidations, and other similar types of corporate restructuring between covered entities, including a division of a covered entity, and to an entity that is not a covered entity but will become a covered entity if the reorganization or sale is completed. Other types of sales of assets, or disclosures to organizations that are not and would not become covered entities, are not included in the definition of health care operations and could only occur if the covered entity obtained valid authorization for such disclosure in accordance with § 164.508 or if the disclosure is otherwise permitted under this rule.

Once a covered entity is sold or merged with another covered entity, the successor in interest becomes responsible for complying with this regulation with respect to the transferred information.

Comment: Several commenters expressed concern that the definition of health care operations failed to include the use of protected health information for the underwriting of new health care policies and took issue with the exclusion of uses and disclosures of protected health information of prospective enrollees. They expressed the concern that limiting health care operations to the underwriting and rating of existing members places a health plan in the position of not being able to evaluate prudently and underwrite a consumer's health care risk.

Response: We agree that covered entities should be able to use the protected health information of prospective enrollees to underwrite and rate new business and change the definition of health care operations accordingly. The definition of health care operations below includes underwriting, premium rating, and other activities related to the creation of a contract of health insurance.

Comment: Several commenters stated that group health plans needed to be able to use and disclose protected health information for purposes of soliciting a contract with a new carrier and rate setting.

Response: We agree and add ''activities relating to the * * * replacement of a contract of insurance'' to cover such disclosures. See § 164.504 for the rules for plan sponsors of group health plans to obtain such information.

Comment: Commenters from the business community supported our recognition of the importance of financial risk transfer mechanisms in the health care marketplace by including ''reinsurance'' in the definition of health care operations. However, they stated that the term ''reinsurance'' alone was not adequate to capture ''stop-loss insurance'' (also referred to as excess of loss insurance), another type of risk transfer insurance.

Response: We agree with the commenters that stop-loss and excess of loss insurance are functionally equivalent to reinsurance and add these to the definition of health care operations.

Comment: Commenters from the employer community explained that there is a trend among employers to contract with a single insurer for all their insurance needs (health, disability, workers' compensation). They stated that in these integrated systems, employee health information is shared among the various programs in the system. The commenters believed the existing definition poses obstacles for those employers utilizing an integrated health system because of the need to obtain authorizations before being permitted to use protected health information from the health plan to administer or audit their disability or workers' compensation plan.

Other commenters representing employers stated that some employers wanted to combine health information from different insurers and health plans providing employee benefits to their workforces, including its group health plan, workers' compensation insurers, and disability insurers, so that they could have more information in order to better manage the occurrences of disability and illness among their workforces. They expressed concern

that the proposed rule would not permit such sharing of information.

Response: While we agree that integrating health information from different benefit programs may produce efficiencies as well as benefits for individuals, the integration also raises significant privacy concerns, particularly if there are no safeguards on uses and disclosures from the integrated data. Under HIPAA, we do not have jurisdiction over many types of insurers that use health information, such as workers' compensation insurers or insurers providing disability income benefits, and we cannot address the extent to which they provide individually identifiable health information to a health plan, nor do we prohibit a health plan from receiving such information. Once a health plan receives identifiable health information, however, the information becomes protected and may only be used and disclosed as otherwise permitted by this rule.

We clarify, however, that a covered entity may provide data and statistical analyses for its customers as a health care operation, provided that it does not disclose protected health information in a way that would otherwise violate this rule. A group health plan or health insurance issuer or HMO, or their business associate on their behalf, may perform such analyses for an employer customer and provide the results in de-identified form to the customer, using integrated data received from other insurers, as long as protected health information is not disclosed in violation of this rule. See the definition of ''health care operations,'' § 164.501. If the employer sponsors more than one group health plan, or if its group health plan provides coverage through more than one health insurance issuer or HMO, the different covered entities may be an organized health care arrangement and be able to jointly participate in such an analysis as part of the health care operations of such organized health care arrangement. See the definitions of ''health care operations'' and ''organized health care arrangement,'' § 164.501. We further clarify that a plan sponsor providing plan administration to a group health plan may participate in such an analysis, provided that the requirements of § 164.504(f) and other parts of this rule are met.

The results described above are the same whether the health information that is being combined is from separate insurers or from one entity that has a health component and also provides excepted benefits. See the discussion relating to health care components, § 164.504.

We note that under the arrangements described above, the final rule provides substantial flexibility to covered entities to provide general data and statistical analyses, resulting in the disclosure of de-identified information, to employers and other customers. An employer also may receive protected health information from a covered entity for any purpose, including those described in comment above, with the authorization of the individual. See § 164.508.

Comment: A number of commenters asserted that the proposed definition appeared to limit training and educational activities to that of health care professionals, students, and trainees. They asked that we expand the definition to include other education-related activities, such as continuing education for providers and training of non-health care professionals as needed for supporting treatment or payment.

Response: We agree with the commenters that the definition of health care operations was unnecessarily limiting with respect to educational activities and expand the definition of health care operations to include ''conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers.'' We clarify that medical rounds are considered treatment, not health care operations.

Comment: A few commenters outlined the need to include the training of non-health care professionals, such as health data analysts, administrators, and computer programmers within the definition of health care operations. It was argued that, in many cases, these professionals perform functions which support treatment and payment and will need access to protected health information in order to carry out their responsibilities.

Response: We agree and expand the definition of health care operations to include training of non-health care professionals.

Comment: One commenter stated that the definition did not explicitly include physician credentialing and peer review.

Response: We have revised the definition to specifically include ''licensing or credentialing activities.'' In addition, peer review activities are captured in the definition as reviewing the competence or qualifications of health care professionals and evaluating practitioner and provider performance.

Health Oversight Agency

Comment: Some commenters sought to have specific organizations defined as health oversight agencies. For example, some commenters asked that the regulation text, rather than the preamble, explicitly list state insurance departments as an example of health oversight agencies. Medical device manufacturers recommended expanding the definition to include government contractors such as coding committees, which provide data to HCFA to help the agency make reimbursement decisions.

One federal agency sought clarification that several of its sub-agencies were oversight agencies; it was concerned about its status in part because the agency fits into more than one of the categories of health oversight agency listed in the proposed rule.

Other commenters recommended expanding the definition of oversight agency to include private-sector accreditation organizations. One commenter recommended stating in the final rule that private companies providing information to insurers and employers are not included in the definition of health oversight agency.

Response: Because the range of health oversight agencies is so broad, we do not include specific examples in the definition. We include many examples in the preamble above and provide further clarity here.

As under the NPRM, state insurance departments are an example of a health oversight agency. A commenter concerned about state trauma registries did not describe the registries' activities or legal charters, so we cannot clarify whether such registries may be health oversight agencies. Government contractors such as coding committees, which provide data to HCFA to support payment processes, are not thereby health oversight agencies under this rule. We clarify that public agencies may fit into more than one category of health oversight agency.

The definition of health oversight agency does not include private-sector accreditation organizations. While their work can promote quality in the health care delivery system, private accreditation organizations are not authorized by law to oversee the health care system or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant. Under the final rule, we consider private accrediting groups to be performing a health care operations function for covered entities. Thus, disclosures to private accrediting organizations are

disclosures for health care operations, not for oversight purposes.

When they are performing accreditation activities for a covered entity, private accrediting organizations will meet the definition of business associate, and the covered entity must enter into a business associate contract with the accrediting organization in order to disclose protected health information. This is consistent with current practice; today, accrediting organizations perform their work pursuant to contracts with the accredited entity. This approach is also consistent with the recommendation by the Joint Commission on Accreditation of Healthcare Organizations and the National Committee for Quality Assurance, which stated in their report titled *Protecting Personal Health Information: A Framework for Meeting the Challenges in a Managed Care Environment* (1998) that ''Oversight organizations, including accrediting bodies, states, and federal agencies, should include in their contracts terms that describe their responsibility to maintain the confidentiality of any personally identifiable health information that they review.''

We agree with the commenter who believed that private companies providing information to insurers and employers are not performing an oversight function; the definition of health oversight agency does not include such companies.

In developing and clarifying the definition of health oversight in the final rule, we seek to achieve a balance in accounting for the full range of activities that public agencies may undertake to perform their health oversight functions while establishing clear and appropriate boundaries on the definition so that it does not become a catch-all category that public and private agencies could use to justify any request for information.

Individual

Comment: A few commenters stated that foreign military and diplomatic personnel, and their dependents, and overseas foreign national beneficiaries, should not be excluded from the definition of ''individual.''

Response: We agree with concerns stated by commenters and eliminate these exclusions from the definition of ''individual'' in the final rule. Special rules for use and disclosure of protected health information about foreign military personnel are stated in § 164.512(k). Under the final rule, protected health information about diplomatic personnel is not accorded special treatment. While the exclusion of overseas foreign national beneficiaries has been deleted from the definition of ''individual,'' we have revised § 164.500 to indicate that the rule does not apply to the Department of Defense or other federal agencies or non-governmental organizations acting on its behalf when providing health care to overseas foreign national beneficiaries. This means that the rule will not cover any health information created incident to the provision of health care to foreign nationals overseas by U.S. sponsored missions or operations. (See § 164.500 and its corresponding preamble for details and the rationale for this policy.)

Comment: Several commenters expressed concern about the interrelationship of the definition of ''individual'' and the two year privacy protection for deceased persons.

Response: In the final rule, we eliminate the two year limit on privacy protection for protected health information about deceased individuals and require covered entities to comply with the requirements of the rule with respect to the protected health information of deceased individuals as long as they hold such information. See discussion under § 164.502.

Individually Identifiable Health Information

Comment: A number of commenters suggested that HHS revise the definitions of health information and individually identifiable health information to include consistent language in paragraph (1) of each respective definition. They observed that paragraph (1) of the definition of health information reads: ''(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse * * *;'' in contrast to paragraph (1) of the definition of individually identifiable health information, which reads: ''(1) Is created by or received from a health care provider, health plan, employer, or health care clearinghouse * * *'' [Emphasis added.]

Another commenter asked that we delete from the definition of health information, the words ''health or'' to make the definition more consistent with the definition of ''health care,'' as well as the words ''whether oral or.''

Response: We define these terms in the final rule as they are defined by Congress in sections 1171(4) and 1171(6) of the Act, respectively. We have, however, changed the word ''from'' in the definition of ''individually identifiable health information'' to conform to the statute.

Comment: Several commenters urged that the definition of individually identifiable health information include information created or received by a researcher. They reasoned that it is important to ensure that researchers using personally identifiable health information are subject to federal privacy standards. They also stated that if information created by a school regarding the health status of its students could be labeled ''health information,'' then information compiled by a clinical researcher regarding an individual also should be considered health information.

Response: We are restricted to the statutory limits of the terms. The Congress did not include information created or received by a researcher in either definition, and, consequently, we do not include such language in the rule's definitions.

Comment: Several commenters suggested modifying the definition of individually identifiable health information to state as a condition that the information provide a direct means of identifying the individual. They commented that the rule should support the need of those (*e.g.,* researchers) who need ''ready access to health information * * * that remains linkable to specific individuals.''

Response: The Congress included in the statutory definition of individually identifiable health information the modifier ''reasonable basis'' when describing the condition for determining whether information can be used to identify the individual. Congress thus intended to go beyond ''direct'' identification and to encompass circumstances in which a reasonable likelihood of identification exists. Even after removing ''direct'' or ''obvious'' identifiers of information, a risk or probability of identification of the subject of the information may remain; in some instances, the risk will not be inconsequential. Thus, we agree with the Congress that ''reasonable basis'' is the appropriate standard to adequately protect the privacy of individuals' health information.

Comment: A number of commenters suggested that the Secretary eliminate the distinction between protected health information and individually identifiable health information. One commenter asserted that all individually identifiable health information should be protected. One commenter observed that the terms individually identifiable health information and protected health information are defined differently in the rule and requested clarification as to the precise scope of coverage of the standards. Another commenter stated

that the definition of individually identifiable health information includes ''employer,'' whereas protected health information pertains only to covered entities for which employers are not included. The commenter argued that this was an ''incongruity'' between the definitions of individually identifiable health information and protected health information and recommended that we remove ''employer'' from the definition of individually identifiable health information.

Response: We define individually identifiable health information in the final rule generally as it is defined by Congress in section 1171(6) of the Act. Because ''employer'' is included in the statutory definition, we cannot accept the comment to remove the word ''employer'' from the regulatory definition.

We use the phrase 'protected health information' to distinguish between the individually identifiable health information that is used or disclosed by the entities that are subject to this rule and the entire universe of individually identifiable health information. 'Individually identifiable health information' as defined in the statute is not limited to health information used or disclosed by covered entities, so the qualifying phrase 'protected health information' is necessary to define that individually identifiable health information to which this rule applies.

Comment: One commenter noted that the definition of individually identifiable health information in the NPRM appeared to be the same definition used in the other HIPAA proposed rule, Security and Electronic Signature Standards (63 FR 43242). However, the commenter stated that the additional condition in the privacy NPRM, that protected health information is or has been electronically transmitted or electronically maintained by a covered entity and includes such information in any other form, appears to create potential disparity between the requirements of the two rules. The commenter questioned whether the provisions in proposed § 164.518(c) were an attempt to install similar security safeguards for such situations.

Response: The statutory definition of individually identifiable health information applies to the entire Administrative Simplification subtitle of HIPAA and, thus, was included in the proposed Security Standards. At this time, however, the final Security Standards have not been published, so the definition of protected health information is relevant only to HIPAA's privacy standards and is, therefore, included in subpart E of part 164 only. We clarify that the requirements in the proposed Security Standards are distinct and separate from the privacy safeguards promulgated in this final rule.

Comment: Several commenters expressed confusion and requested clarification as to what is considered health information or individually identifiable health information for purposes of the rule. For example, one commenter was concerned that information exists in collection agencies, credit bureaus, etc., which could be included under the proposed regulation but may or may not have been originally obtained by a covered entity. The commenter noted that generally this information is not clinical, but it could be inferred from the data that a health care provider provided a person or member of person's family with health care services. The commenter urged the Secretary to define more clearly what and when information is covered.

One commenter queried how a non-medical record keeper could tell when personal information is health information within the meaning of rule, *e.g.,* when a worker asks for a low salt meal in a company cafeteria, when a travel voucher of an employee indicates that the traveler returned from an area that had an outbreak of fever, or when an airline passenger requests a wheel chair. It was suggested that the rule cover health information in the hands of schools, employers, and life insurers only when they receive individually identifiable health information from a covered entity or when they create it while providing treatment or making payment.

Response: This rule applies only to individually identifiable health information that is held by a covered entity. Credit bureaus, airlines, schools, and life insurers are not covered entities, so the information described in the above comments is not protected health information. Similarly, employers are not covered entities under the rule. Covered entities must comply with this regulation in their health care capacity, not in their capacity as employers. For example, information in hospital personnel files about a nurses' sick leave is not protected health information under this rule.

Comment: One commenter recommended that the privacy of health information should relate to actual medical records. The commenter expressed concern about the definition's broadness and contended that applying prescriptive rules to information that health plans hold will not only delay processing of claims and coverage decisions, but ultimately affect the quality and cost of care for health care consumers.

Response: We disagree. Health information about individuals exists in many types of records, not just the formal medical record about the individual. Limiting the rule's protections to individually identifiable health information contained in medical records, rather than individually identifiable health information in any form, would omit a significant amount of individually identifiable health information, including much information in covered transactions.

Comment: One commenter voiced a need for a single standard for individually identifiable health information and disability and workers' compensation information; each category of information is located in their one electronic data base, but would be subjected to a different set of use and transmission rules.

Response: We agree that a uniform, comprehensive privacy standard is desirable. However, our authority under the HIPAA is limited to individually identifiable health information as it is defined in the statute. The legislative history of HIPAA makes clear that workers' compensation and disability benefits programs were not intended to be covered by the rule. Entities are of course free to apply the protections required by this rule to all health information they hold, including the excepted benefits information, if they wish to do so (for example, in order to reduce administrative burden).

Comment: Commenters recommended that the definition of individually identifiable health information not include demographic information that does not have any additional health, treatment, or payment information with it. Another commenter recommended that protected health information should not include demographic information at all.

Response: Congress explicitly included demographic information in the statutory definition of this term, so we include such language in our regulatory definition of it.

Comments: A number of commenters expressed concern about whether references to personal information about individuals, such as ''John Doe is fit to work as a pipe fitter * * *'' or ''Jane Roe can stand no more than 2 hours * * *'', would be considered individually identifiable health information. They argued that such ''fitness-to-work'' and ''fitness for duty'' statements are not health care because they do not reveal the type of

information (such as the diagnosis) that is detrimental to an individual's privacy interest in the work environment.

Response: References to personal information such as those suggested by the commenters could be individually identifiable health information if the references were created or received by a health care provider, health plan, employer, or health care clearinghouse and they related to the past, present, or future physical or mental health or condition, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual. Although these fitness for duty statements may not reveal a diagnosis, they do relate to a present physical or mental condition of an individual because they describe the individual's capacity to perform the physical and mental requirements of a particular job at the time the statement is made (even though there may be other non-health-based qualifications for the job). If these statements were created or received by one of more of the entities described above, they would be individually identifiable health information.

Law Enforcement Official

Comment: Some commenters, particularly those representing health care providers, expressed concern that the proposed definition of ''law enforcement official'' could have allowed many government officials without health care oversight duties to obtain access to protected health information without patient consent.

Response: We do not intend for the definition of ''law enforcement official'' to be limited to officials with responsibilities directly related to health care. Law enforcement officials may need protected health information for investigations or prosecutions unrelated to health care, such as investigations of violent crime, criminal fraud, or crimes committed on the premises of health care providers. For these reasons, we believe it is not appropriate to limit the definition of ''law enforcement official'' to persons with responsibilities of oversight of the health care system.

Comment: A few commenters expressed concern that the proposed definition could include any county or municipal official, even those without traditional law enforcement training.

Response: We do not believe that determining training requirements for law enforcement officials is appropriately within the purview of this regulation; therefore, we do not make the changes that these commenters requested.

Comment: Some commenters, particularly those from the district attorney community, expressed general concern that the proposed definition of ''law enforcement official'' was too narrow to account for the variation in state interpretations of law enforcement officials' power. One group noted specifically that the proposed definition could have prevented prosecutors from gaining access to needed protected health information.

Response: We agree that protected health information may be needed by law enforcement officials for both investigations and prosecutions. We did not intend to exclude the prosecutorial function from the definition of ''law enforcement official,'' and accordingly we modify the definition of law enforcement official to reflect their involvement in prosecuting cases. Specifically, in the final rule, we define law enforcement official as an official of any agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, who is empowered by law to: (1) Investigate or conduct an inquiry into a potential violation of law; or (2) prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Comment: One commenter recommended making the definition of law enforcement official broad enough to encompass Medicaid program auditors, because some matters requiring civil or criminal law enforcement action are first identified through the audit process.

Response: We disagree. Program auditors may obtain protected health information necessary for their audit functions under the oversight provision of this regulation (§ 164.512(d)).

Comment: One commenter suggested that the proposed definition of ''law enforcement official'' could be construed as limited to circumstances in which an official ''knows'' that law has been violated. This commenter was concerned that, because individuals are presumed innocent and because many investigations, such as random audits, are opened without an agency knowing that there is a violation, the definition would not have allowed disclosure of protected health information for these purposes. The commenter recommended modifying the definition to include investigations into ''whether'' the law has been violated.

Response: We do not intend for lawful disclosures of protected health information for law enforcement purposes to be limited to those in which a law enforcement official knows that law has been violated. Accordingly, we revise the definition of ''law enforcement official'' to include investigations of ''potential'' violations of law.

Marketing

Comments related to ''marketing'' are addressed in the responses to comments regarding § 164.514(e).

Payment

Comment: One commenter urged that the Department not permit protected health information to be disclosed to a collection agency for collecting payment on a balance due on patient accounts. The commenter noted that, at best, such a disclosure would only require the patient's and/or insured's address and phone number.

Response: We disagree. A collection agency may require additional protected health information to investigate and assess payment disputes for the covered entity. For example, the collection agency may need to know what services the covered entity rendered in order to resolve disputes about amounts due. The information necessary may vary, depending on the nature of the dispute. Therefore we do not specify the information that may be used or disclosed for collection activities. The commenter's concern may be addressed by the minimum necessary requirements in § 164.514. Under those provisions, when a covered entity determines that a collection agency only requires limited information for its activities, it must make reasonable efforts to limit disclosure to that information.

Comment: A number of commenters supported retaining the expansive definition in the proposed rule so that current methods of administering the claims payment process would not be hindered by blocking access to protected health information.

Response: We agree and retain the proposed overall approach to the definition.

Comment: Some commenters argued that the definition of ''payment'' should be narrowly interpreted as applying only to the individual who is the subject of the information.

Response: We agree with the commenter and modify the definition to clarify that payment activities relate to the individual to whom health care is provided.

Comment: Another group of commenters asserted that the doctor-patient relationship was already being interfered with by the current practices of managed care. For example, it was argued that the definition expanded the

power of government and other third party ''payors,'' turning them into controllers along with managed care companies. Others stated that activities provided for under the definition occur primarily to fulfill the administrative function of managed health plans and that an individual's privacy is lost when his or her individually identifiable health information is shared for administrative purposes.

Response: Activities we include in the definition of payment reflect core functions through which health care and health insurance services are funded. It would not be appropriate for a rule about health information privacy to hinder mechanisms by which health care is delivered and financed. We do not through this rule require any health care provider to disclose protected health information to governmental or other third party payors for the activities listed in the payment definition. Rather, we allow these activities to occur, subject to and consistent with the requirements of this rule.

Comment: Several commenters requested that we expand the definition to include ''coordination of benefits'' as a permissible activity.

Response: We agree and modify the definition accordingly.

Comment: A few commenters raised concerns that the use of ''medical data processing'' was too restrictive. It was suggested that a broader reference such as ''health related'' data processing would be more appropriate.

Response: We agree and modify the definition accordingly.

Comment: Some commenters suggested that the final rule needed to clarify that drug formulary administration activities are payment related activities.

Response: While we agree that uses and disclosures of protected health information for drug formulary administration and development are common and important activities, we believe these activities are better described as health care operations and that these activities come within that definition.

Comment: Commenters asked that the definition include calculation of prescription drug costs, drug discounts, and maximum allowable costs and copayments.

Response: Calculations of drug costs, discounts, or copayments are payment activities if performed with respect to a specific individual and are health care operations if performed in the aggregate for a group of individuals.

Comment: We were urged to specifically exclude ''therapeutic substitution'' from the definition.

Response: We reject this suggestion. While we understand that there are policy concerns regarding therapeutic substitution, those policy concerns are not primarily about privacy and thus are not appropriately addressed in this regulation.

Comment: A few commenters asked that patient assistance programs (PAPS) should be excluded from the definition of payment. Such programs are run by or on behalf of manufacturers and provide free or discounted medications to individuals who could not afford to purchase them. Commenters were concerned that including such activities in the definition of payment could harm these programs.

For example, a university school of pharmacy may operate an outreach program and serve as a clearinghouse for information on various pharmaceutical manufacturer PAPS. Under the program state residents can submit a simple application to the program (including medication regimen and financial information), which is reviewed by program pharmacists who study the eligibility criteria and/or directly call the manufacturer's program personnel to help evaluate eligibility for particular PAPS. The program provides written guidance to the prescribing physicians that includes a suggested approach for helping their indigent patients obtain the medications that they need and enrollment information for particular PAPS.

Response: We note that the concerns presented are not affected by definition of ''payment.'' The application of this rule to patient assistance programs activities will depend on how the individual programs operate and are affected primarily by the definition of treatment. Each of these programs function differently, so it is not possible to state a blanket rule for whether and how the rule affects such programs.

Under the example provided, the physician who contacts the program on behalf of a patient is managing the patient's care. If the provider is also a covered entity, he or she would be permitted to make such a ''treatment'' disclosure of protected health information if a general consent had been obtained from the patient. Depending on the particular facts, the manufacturer, by providing the prescription drugs for an individual, could also be providing health care under this rule. Even so, however, the manufacturer may or may not be a covered entity, depending on whether or not it engages in any of the standard electronic transactions (See the definition of a covered entity). It also may be an indirect treatment provider, since it may be providing the product through another provider, not directly to the patient. In this example, the relevant disclosures of protected health information by any covered health care provider with a direct treatment relationship with the patient would be permitted subject to the general consent requirements of § 164.506.

Whether and how this rule affects the school of pharmacy is equally dependent on the specific facts. For example, if the school merely provides a patient or a physician with the name of a manufacturer and a contact phone number, it would not be functioning as a health care provider and would not be subject to the rule. However, if the school is more involved in the care of the individual, its activities could come in within the definition of ''health care provider'' under this rule.

Comment: Commenters pointed out that drugs may or may not be ''covered'' under a plan. Individuals, on the other hand, may or may not be ''eligible'' for benefits under a plan. The definition should incorporate both terms to clarify that determinations of both coverage and eligibility are payment activities.

Response: We agree and modify the rule to include ''eligibility''.

Comment: Several commenters urged that ''concurrent and retrospective review'' were significant utilization review activities and should be incorporated.

Response: We agree and modify the definition accordingly.

Comment: Commenters noted that the proposed rule was not clear as to whether protected health information could be used to resolve disputes over coverage, including appeals or complaints regarding quality of care.

Response: We modify the definition of payment to include resolution of payment and coverage disputes; the final definition of payment includes ''the adjudication * * * of health benefit claims.'' The other examples provided by commenters, such as arranging, conducting, or assistance with primary and appellate level review of enrollee coverage appeals, also fall within the scope of adjudication of health benefits claims. Uses and disclosures of protected health information to resolve disputes over quality of care may be made under the definition of ''health care operations'' (see above).

Comment: Some commenters suggested that if an activity falls within the scope of payment it should not be considered marketing. Commenters supported an approach that would bar such an activity from being construed as ''marketing'' even if performing that

activity would result in financial gain to the covered entity.

Response: We agree that the proposed rule did not clearly define ''marketing,'' leaving commenters to be concerned about whether payment activities that result in financial gain might be considered marketing. In the final rule we add a definition of marketing and clarify when certain activities that would otherwise fall within that definition can be accomplished without authorization. We believe that these changes will clarify the distinction between marketing and payment and address the concerns raised by commenters.

Comment: Commenters asserted that HHS should not include long-term care insurance within the definition of ''health plan.'' If they are included, the commenters argued that the definition of payment must be modified to reflect the activities necessary to support the payment of long-term care insurance claims. As proposed, commenters argued that the definition of payment would not permit long term care insurers to use and disclose protected health information without authorization to perform functions that are ''compatible with and directly relate to * * * payment'' of claims submitted under long term care policies.

Response: Long-term care policies, except for nursing home fixed-indemnity policies, are defined as health plans by the statute (see definition of ''health plan,'' above). We disagree with the assertion that the definition of payment does not permit long term care insurers to undertake these necessary activities. Processing of premium payments, claims administration, and other activities suggested for inclusion by the commenters are covered by the definition. The rule permits protected health information to be used or disclosed by a health plan to determine or fulfill its responsibility for provision of benefits under the health plan.

Comment: Some commenters argued that the definition needs to be expanded to include the functions of obtaining stop-loss and ceding reinsurance.

Response: We agree that use and disclosure of protected health information for these activities should be permitted without authorization, but have included them under health care operation rather than payment.

Comment: Commenters asked that the definition be modified to include collection of accounts receivable or outstanding accounts. Commenters raised concern that the proposed rule, without changes, might unintentionally prevent the flow of information between medical providers and debt collectors.

Response: We agree that the proposed definition of payment did not explicitly provide for ''collection activities'' and that this oversight might have impeded a covered entity's debt collection efforts. We modify the regulatory text to add ''collection activities.''

Comment: The preamble should clarify that self-insured group health and workers' compensation plans are not covered entities or business partners.

Response: The statutory definition of health plan does not include workers' compensation products. See the discussion of ''health plan'' under § 160.103 above.

Comment: Certain commenters explained that third party administrators usually communicate with employees through Explanation of Benefit (EOB) reports on behalf of their dependents (including those who might not be minor children). Thus, the employee might be apprised of the medical encounters of his or her dependents but not of medical diagnoses unless there is an over-riding reason, such as a child suspected of drug abuse due to multiple prescriptions. The commenters urged that the current claim processing procedures be allowed to continue.

Response: We agree. We interpret the definition of payment and, in particular the term ''claims management,'' to include such disclosures of protected health information.

Comment: One private company noted that pursuant to the proposed Transactions Rule standard for payment and remittance advice, the ASC X12N 835 can be used to make a payment, send a remittance advice, or make a payment and send remittance advice by a health care payor and a health care provider, either directly or through a designated financial institution. Because a remittance advice includes diagnostic or treatment information, several private companies and a few public agencies believed that the proposed Transactions Rule conflicted with the proposed privacy rule. Two health plans requested guidance as to whether, pursuant to the ASC X12N 835 implementation guide, remittance advice information is considered ''required'' or ''situational.'' They sought guidance on whether covered entities could include benefits information in payment of claims and transfer of remittance information.

One commenter asserted that if the transmission of certain protected health information were prohibited, health plans may be required to strip remittance advice information from the ASC X12N 835 when making health care payments. It recommended modifying the proposed rule to allow covered entities to provide banks or financial institutions with the data specified in any transaction set mandated under the Transactions Rule for health care claims payment.

Similarly, a private company and a state health data organization recommended broadening the scope of permissible disclosures pursuant to the banking section to include integrated claims processing information, as contained in the ASC X12N 835 and proposed for adoption in the proposed Transactions Rule; this transaction standard includes diagnostic and treatment information. The company argued that inclusion of diagnostic and treatment information in the data transmitted in claims processing was necessary for comprehensive and efficient integration in the provider's patient accounting system of data corresponding with payment that financial institutions credit to the provider's account.

A state health data organization recommended applying these rules to financial institutions that process electronic remittance advice pursuant to the Transactions Rule.

Response: The Transactions Rule was published August 17, 2000, after the issuance of the privacy proposed rule. As noted by the commenters, the ASC X12N 835 we adopted as the ''Health Care Payment and Remittance Advice'' standard in the Transactions Rule has two parts. They are the electronic funds transfer (EFT) and the electronic remittance advice (ERA). The EFT part is optional and is the mechanism that payors use to electronically instruct one financial institution to move money from one account to another at the same or at another financial institution. The EFT includes information about the payor, the payee, the amount, the payment method, and a reassociation trace number. Since the EFT is used to initiate the transfer of funds between the accounts of two organizations, typically a payor to a provider, it includes no individually identifiable health information, not even the names of the patients whose claims are being paid. The funds transfer information may also be transmitted manually (by check) or by a variety of other electronic means, including various formats of electronic transactions sent through a payment network, such as the Automated Clearing House (ACH) Network.

The ERA, on the other hand, contains specific information about the patients and the medical procedures for which

the money is being paid and is used to update the accounts receivable system of the provider. This information is always needed to complete a standard Health Care Payment and Remittance Advice transaction, but is never needed for the funds transfer activity of the financial institution. The only information the two parts of this transaction have in common is the reassociation trace number.

Under the ASC X12N 835 standard, the ERA may be transmitted alone, directly from the health plan to the health care provider and the reassociation trace number is used by the provider to match the ERA information with a specific payment conducted in some other way (e.g., EFT or paper check). The standard also allows the EFT to be transmitted alone, directly to the financial institution that will initiate the payment. It also allows both parts to be transmitted together, even though the intended recipients of the two parts are different (the financial institution and the provider). For example, this would be done when the parties agree to use the ACH system to carry the ERA through the provider's bank to the provider when it is more efficient than sending the ERA separately through a different electronic medium.

Similarly, the ASC X12N 820 standard for premium payments has two parts, an EFT part (identical to that of the 835) and a premium data part containing identity and health information about the individuals for whom health insurance premiums are being paid.

The transmission of both parts of the standards are payment activities under this rule, and permitted subject to certain restrictions. Because a financial institution does not require the remittance advice or premium data parts to conduct funds transfers, disclosure of those parts by a covered entity to it (absent a business associate arrangement to use the information to conduct other activities) would be a violation of this rule.

We note that additional requirements may be imposed by the final Security Rule. Under the proposed Security Rule, the ACH system and similar systems would have been considered ''open networks'' because transmissions flow unpredictably through and become available to member institutions who are not party to any business associate agreements (in a way similar to the internet). The proposed Security Rule would require any protected health information transferred through the ACH or similar system to be encrypted.

Comment: A few commenters noted the Gramm-Leach-Bliley (GLB) Act (Pub. L. 106–102) allows financial holding companies to engage in a variety of business activities, such as insurance and securities, beyond traditional banking activities. Because the term ''banking'' may take on broader meaning in light of these changes, the commenter recommended modifying the proposed rule to state that disclosure of diagnostic and treatment information to banks along with payment information would constitute a violation of the rule. Specifically, the organization recommended clarifying in the final rule that the provisions included in the proposed section on banking and payment processes (proposed § 164.510(i)) govern payment processes only and that all activities of financial institutions that did not relate directly to payment processes must be conducted through business partner contracts. Furthermore, this group recommended clarifying that if financial institutions act as payors, they will be covered entities under the rule.

Response: We recognize that implementation of the GLB Act will expand significantly the scope of activities in which financial holding companies engage. However, unless a financial institution also meets the definition of a ''covered entity,'' it cannot be a covered entity under this rule.

We agree with the commenters that disclosure of diagnostic and specific treatment information to financial institutions for many banking and funds processing purposes may not be consistent with the minimum necessary requirements of this final rule. We also agree with the commenters that financial institutions are business associates if they receive protected health information when they engage in activities other than funds processing for covered entities. For example, if a health care provider contracts with a financial institution to conduct ''back office'' billing and accounts receivable activities, we require the provider to enter into a business associate contract with the institution.

Comment: Two commenters expressed support for the proposed rule's approach to disclosure for banking and payment processes. On the other hand, many other commenters were opposed to disclosure of protected health information without authorization to banks. One commenter said that no financial institution should have individually identifiable health information for any reason, and it said there were technological means for separating identity from information necessary for financial transactions. Some commenters believed that implementation of the proposed rule's banking provisions could lead banks to deny loans on the basis of individuals' health information.

Response: We seek to achieve a balance between protecting patient privacy and facilitating the efficient operation of the health care system. While we agree that financial institutions should not have access to extensive information about individuals' health, we recognize that even the minimal information required for processing of payments may effectively reveal a patient's health condition; for example, the fact that a person has written a check to a provider suggests that services were rendered to the person or a family member. Requiring authorization for disclosure of protected health information to a financial institution in order to process every payment transaction in the health care system would make it difficult, if not impossible, for the health care system to operate effectively. See also discussion of section 1179 of the Act above.

Comment: Under the proposed rule, covered entities could have disclosed the following information without consent to financial institutions for the purpose of processing payments: (1) The account holder's name and address; (2) the payor or provider's name and address; (3) the amount of the charge for health services; (4) the date on which services were rendered; (5) the expiration date for the payment mechanism, if applicable (e.g., credit card expiration date); and (6) the individual's signature. The proposed rule solicited comments on whether additional data elements would be necessary to process payment transactions from patients to covered entities.

One commenter believed that it was unnecessary to include this list in the final rule, because information that could have been disclosed under the proposed minimum necessary rule would have been sufficient to process banking and payment information. Another private company said that its extensive payment systems experience indicated that we should avoid attempts to enumerate a list of information allowed to be disclosed for banking and payment processing. Furthermore, the commenter said, the proposed rule's list of information allowed to be disclosed was not sufficient to perform the range of activities necessary for the operation of modern electronic payment systems. Finally, the commenter said, inclusion of specific data elements allowed to be

disclosed for banking and payment processes rule would stifle innovation in continually evolving payment systems. Thus, the commenter recommended that in the final rule, we eliminate the minimum necessary requirement for banking and payment processing and that we do not include a list of specific types of information allowed to be disclosed for banking and payment processes.

On the other hand, several other commenters supported applying the minimum necessary standard to covered entities' disclosures to financial institutions for payment processing. In addition, these groups said that because financial institutions are not covered entities under the proposed rule, they urged Congress to enact comprehensive privacy legislation to limit financial institutions' use and re-disclosure of the minimally necessary protected health information they could receive under the proposed rule. Several of these commenters said that, in light of the increased ability to manipulate data electronically, they were concerned that financial institutions could use the minimal protected health information they received for making financial decisions. For example, one of these commenters said that a financial institution could identify an individual who had paid for treatment of domestic violence injuries and subsequently could deny the individual a mortgage based on that information.

Response: We agree with the commenters who were concerned that a finite list of information could hamper systems innovation, and we eliminate the proposed list of data items. However, we disagree with the commenters who argued that the requirement for minimum necessary disclosures not apply to disclosures to financial institution or for payment activities. They presented no persuasive reasons why these disclosures differ from others to which the standard applies, nor did they suggest alternative means of protecting individuals' privacy. Further, with elimination of the proposed list of items that may be disclosed, it will be necessary to rely on the minimum necessary disclosure requirement to ensure that disclosures for payment purposes do not include information unnecessary for that purposes. In practice, the following is the information that generally will be needed: the name and address of the individual; the name and address of the payor or provider; the amount of the charge for health services; the date on which health services were rendered; the expiration date for the payment mechanism, if applicable (i.e., credit card expiration date); the individual's signature; and relevant identification and account numbers.

Comment: One commenter said that the minimum necessary standard would be impossible to implement with respect to information provided on its standard payment claim, which, it said, was used by pharmacies for concurrent drug utilization review and that was expected to be adopted by HHS as the national pharmacy payment claim.

Two other commenters also recommended clarifying in the final rule that pharmacy benefit cards are not considered a type of ''other payment card'' pursuant to the rule's provisions governing payment processes. These commenters were concerned that if pharmacy benefit cards were covered by the rule's payment processing provisions, their payment claim, which they said was expected to be adopted by HHS as the national pharmacy payment claim, may have to be modified to comply with the minimum necessary standard that would have been required pursuant to proposed § 164.510(i) on banking and payment processes. One of these commenters noted that its payment claim facilitates concurrent drug utilization review, which was mandated by Congress pursuant to the Omnibus Budget Reconciliation Act of 1990 and which creates the real-time ability for pharmacies to gain access to information that may be necessary to meet requirements of this and similar state laws. The commenter said that information on its standard payment claim may include information that could be used to provide professional pharmacy services, such as compliance, disease management, and outcomes programs. The commenter opposed restricting such information by applying the minimum necessary standard.

Response: We make an exception to the minimum necessary disclosure provision of this rule for the required and situational data elements of the standard transactions adopted in the Transactions Rule, because those elements were agreed to through the ANSI-accredited consensus development process. The minimum necessary requirements do apply to optional elements in such standard transactions, because industry consensus has not resulted in precise and unambiguous situation specific language to describe their usage. This is particularly relevant to the NCPDP standards for retail pharmacy transactions referenced by these commenters, in which the current standard leaves most fields optional. For this reason, we do not accept this suggestion.

The term 'payment card' was intended to apply to a debit or credit card used to initiate payment transactions with a financial institution. We clarify that pharmacy benefit cards, as well as other health benefit cards, are used for identification of individual, plan, and benefits and do not qualify as ''other payment cards.''

Comment: Two commenters asked the following questions regarding the banking provisions of the proposed rule: (1) Does the proposed regulation stipulate that disclosures to banks and financial institutions can occur only once a patient has presented a check or credit card to the provider, or pursuant to a standing authorization?; and (2) Does the proposed rule ban disclosure of diagnostic or other related detailed payment information to financial institutions?

Response: We do not ban disclosure of diagnostic information to financial institutions, because some such information may be evident simply from the name of the payee (e.g., when payment is made to a substance abuse clinic). This type of disclosure, however, is permitted only when reasonably necessary for the transaction (see requirements for minimum necessary disclosure of protected health information, in § 164.502 and § 164.514).

Similarly, we do not stipulate that such disclosure may be made only once a patient has presented a check or credit card, because some covered entities hire financial institutions to perform services such as management of accounts receivables and other back office functions. In providing such services to covered entities, the financial institution will need access to protected health information. (In this situation, the disclosure will typically be made under a business associate arrangement that includes provisions for protection of the information.)

Comment: One commenter was concerned that the proposed rule's section on financial institutions, when considered in conjunction with the proposed definition of ''protected health information,'' could have been construed as making covered entities' disclosures of consumer payment history information to consumer reporting agencies subject to the rule. It noted that covered entities' reporting of payment history information to consumer reporting agencies was not explicitly covered by the proposed rule's provisions regarding disclosure of protected health information without authorization. It was also concerned that the proposed rule's minimum necessary standard could have been interpreted to

prevent covered entities and their business partners from disclosing appropriate and complete information to consumer reporting agencies. As a result, it said, consumer reporting agencies might not be able to compile complete consumer reports, thus potentially creating an inaccurate picture of a consumer's credit history that could be used to make future credit decisions about the individual.

Furthermore, this commenter said, the proposed rule could have been interpreted to apply to any information disclosed to consumer reporting agencies, thus creating the possibility for conflicts between the rule's requirements and those of the Fair Credit Reporting Act. They indicated that areas of potential overlap included: limits on subsequent disclosures; individual access rights; safeguards; and notice requirements.

Response: We have added to the definition of ''payment'' disclosure of certain information to consumer reporting agencies. With respect to the remaining concerns, this rule does not apply to consumer reporting agencies if they are not covered entities.

Comment: Several commenters recommended prohibiting disclosure of psychotherapy notes under this provision and under all of the sections governing disclosure without consent for national priority purposes.

Response: We agree that psychotherapy notes should not be disclosed without authorization for payment purposes, and the final rule does not allow such disclosure. See the discussion under § 164.508.

Protected Health Information

Comment: An overwhelmingly large number of commenters urged the Secretary to expand privacy protection to all individually identifiable health information, regardless of form, held or transmitted by a covered entity. Commenters provided many arguments in support of their position. They asserted that expanding the scope of covered information under the rule would increase patient confidence in their health care providers and the health care system in general. Commenters stated that patients may not seek care or honestly discuss their health conditions with providers if they do not believe that all of their health information is confidential. In particular, many suggested that this fear would be particularly strong with certain classes of patients, such as persons with disabilities, who may be concerned about potential discrimination, embarrassment or stigmatization, or domestic violence victims, who may hide the real cause of their injuries.

In addition, commenters felt that a more uniform standard that covered all records would reduce the complexity, burden, cost, and enforcement problems that would result from the NPRM's proposal to treat electronic and non-electronic records differently. Specifically, they suggested that such a standard would eliminate any confusion regarding how to treat mixed records (paper records that include information that has been stored or transmitted electronically) and would eliminate the need for health care providers to keep track of which portions of a paper record have been (or will be) stored or transmitted electronically, and which are not. Many of these commenters argued that limiting the definition to information that is or has at one time been electronic would result in different protections for electronic and paper records, which they believe would be unwarranted and give consumers a false sense of security. Other comments argued that the proposed definition would cause confusion for providers and patients and would likely cause difficulties in claims processing. Many others complained about the difficulty of determining whether information has been maintained or transmitted electronically. Some asked us to explicitly list the electronic functions that are intended to be excluded, such as voice mail, fax, etc. It was also recommended that the definitions of ''electronic transmission'' and ''electronic maintenance'' be deleted. It was stated that the rule may apply to many medical devices that are regulated by the FDA. A commenter also asserted that the proposal's definition was technically flawed in that computers are also involved in analog electronic transmissions such as faxes, telephone, etc., which is not the intent of the language. Many commenters argued that limiting the definition to information that has been electronic would create a significant administrative burden, because covered entities would have to figure out how to apply the rule to some but not all information.

Others argued that covering all individually identifiable health information would eliminate any disincentives for covered entities to convert from paper to computerized record systems. These commenters asserted that under the proposed limited coverage, contrary to the intent of HIPAA's administrative simplification standards, providers would avoid converting paper records into computerized systems in order to bypass the provisions of the regulation. They argued that treating all records the same is consistent with the goal of increasing the efficiency of the administration of health care services.

Lastly, in the NPRM, we explained that while we chose not to extend our regulatory coverage to all records, we did have the authority to do so. Several commenters agreed with our interpretation of the statute and our authority and reiterated such statements in arguing that we should expand the scope of the rule in this regard.

Response: We find these commenters' arguments persuasive and extend protections to individually identifiable health information transmitted or maintained by a covered entity in any form (subject to the exception for ''education records'' governed by FERPA and records described at 20 U.S.C. 1232g(a)(4)(B)(iv)). We do so for the reasons described by the commenters and in our NPRM, as well as because we believe that the approach in the final rule creates a logical, consistent system of protections that recognizes the dynamic nature of health information use and disclosure in a continually shifting health care environment. Rules that are specific to certain formats or media, such as ''electronic'' or ''paper,'' cannot address the privacy threats resulting from evolving forms of data capture and transmission or from the transfer of the information from one form to another. This approach avoids the somewhat artificial boundary issues that stem from defining what is and is not electronic.

In addition, we have reevaluated our reasons for not extending privacy protections to all paper records in the NPRM and after review of comments believe such justifications to be less compelling than we originally thought. For example, in the NPRM, we explained that we chose not to cover all paper records in order to focus on the public concerns about health information confidentiality in electronic communications, and out of concern that the potential additional burden of covering all records may not be justified because of the lower privacy risks presented by records that are in paper form only. As discussed above however, a great many commenters asserted that dealing with a mixture of protected and non-protected records is more burdensome, and that public concerns over health information confidentiality are not at all limited to electronic communications.

We note that medical devices in and of themselves, for example, pacemakers, are not protected health information for purposes of this regulation. However, information in or from the device may

be protected health information to the extent that it otherwise meets the definition.

Comment: Numerous commenters argued that the proposed coverage of any information other than that which is transmitted electronically and/or in a HIPAA transaction exceeds the Secretary's authority under section 264(c)(1) of HIPAA. The principal argument was that the initial language in section 264(c)(1) (''If language governing standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a) of the Social Security Act * * * is not enacted by [August 21, 1999], the Secretary * * * shall promulgate final regulations containing such standards* * *'') limits the privacy standards to ''information transmitted in connection with the [HIPAA] transactions.'' The precise argument made by some commenters was that the grant of authority is contained in the words ''such standards,'' and that the referent of that phrase was ''standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a)* * *''.

Commenters also argued that this limitation on the Secretary's authority is discernible from the statutory purpose statement at section 261 of HIPAA, from the title to section 1173(a) (''Standards to Enable Electronic Exchange''), and from various statements in the legislative history, such as the statement in the Conference Report that the ''Secretary would be required to establish standards and modifications to such standards regarding the privacy of individually identifiable health information that is in the health information network.'' H. Rep. No. 104–736,104th Cong., 2d Sess., at 265. It was also argued that extension of coverage beyond the HIPAA transactions would be inconsistent with the underlying statutory trade-off between facilitating accessibility of information in the electronic transactions for which standards are adopted under section 1173(a) and protecting that information through the privacy standards.

Other commenters argued more generally that the Secretary's authority was limited to information in electronic form only, not information in any other form. These comments tended to focus on the statutory concern with regulating transactions in electronic form and argued that there was no need to have the privacy standards apply to information in paper form, because there is significantly less risk of breach of privacy with respect to such information.

The primary justifications provided by commenters for restricting the scope of covered individually identifiable health information under the regulation were that such an approach would reduce the complexity, burden, cost, and enforcement problems that would result from a rule that treats electronic and non-electronic records differently; would appropriately limit the rule's focus to the security risks that are inherent in electronic transmission or maintenance of individually identifiable health information; and would conform these provisions of the rule more closely with their interpretation of the HIPAA statutory language.

Response: We disagree with these commenters. We believe that restricting the scope of covered information under the rule consistent with any of the comments described above would generate a number of policy concerns. Any restriction in the application of privacy protections based on the media used to maintain or transmit the information is by definition arbitrary, unrelated to the potential use or disclosure of the information itself and therefore not responsive to actual privacy risks. For example, information contained in a paper record may be scanned and transmitted worldwide almost as easily as the same information contained in an electronic claims transaction, but would potentially not be protected.

In addition, application of the rule to only the standard transactions would leave large gaps in the amount of health information covered. This limitation would be particularly harmful for information used and disclosed by health care providers, who are likely to maintain a great deal of information never contained in a transaction.

We disagree with the arguments that the Secretary lacks legal authority to cover all individually identifiable health information transmitted or maintained by covered entities. The arguments raised by these comments have two component parts: (1) That the Secretary's authority is limited by form, to individually identifiable health information in electronic form only; and (2) that the Secretary's authority is limited by content, to individually identifiable health information that is contained in what commenters generally termed the ''HIPAA transactions,'' i.e., information contained in a transaction for which a standard has been adopted under section 1173(a) of the Act.

With respect to the issue of form, the statutory definition of ''health information'' at section 1171(4) of the Act defines such information as ''any information, *whether oral or recorded in any form or medium*'' (emphasis added) which is created or received by certain entities and relates to the health condition of an individual or the provision of health care to an individual (emphasis added). ''Individually identifiable health information'', as defined at section 1171(6) of the Act, is information that is created or received by a subset of the entities listed in the definition of ''health information'', relates to the same subjects as ''health information,'' and is, in addition, individually identifiable. Thus, ''individually identifiable health information'' is, as the term itself implies, a subset of ''health information.'' As ''health information,'' ''individually identifiable health information'' means, among other things, information that is ''oral or recorded in any form or medium.'' Therefore, the statute does not limit ''individually identifiable health information'' to information that is in electronic form only.

With respect to the issue of content, the limitation of the Secretary's authority to information in HIPAA transactions under section 264(c)(1) is more apparent than real. While the first sentence of section 264(c)(1) may be read as limiting the regulations to standards with respect to the privacy of individually identifiable health information ''transmitted in connection with the [HIPAA] transactions,'' what that sentence in fact states is that the privacy regulations must ''contain'' such standards, not be limited to such standards. The first sentence thus sets a statutory minimum, first for Congress, then for the Secretary. The second sentence of section 264(c)(1) directs that the regulations ''address at least the subjects in subsection (b) (of section 264).'' Section 264(b), in turn, refers only to ''individually identifiable health information'', with no qualifying language, and refers back to subsection (a) of section 264, which is not limited to HIPAA transactions. Thus, the first and second sentences of section 264(c)(1) can be read as consistent with each other, in which case they direct the issuance of privacy standards with respect to individually identifiable health information. Alternatively, they can be read as ambiguous, in which case one must turn to the legislative history.

The legislative history of section 264 does not reflect the content limitation of the first sentence of section 264(c)(1). Rather, the Conference Report

summarizes this section as follows: ''If Congress fails to enact privacy legislation, the Secretary is required to develop standards with respect to privacy of individually identifiable health information not later than 42 months from the date of enactment.'' *Id.*, at 270. This language indicates that the overriding purpose of section 264(c)(1) was to postpone the Secretary's duty to issue privacy standards (which otherwise would have been controlled by the time limits at section 1174(a)), in order to give Congress more time to pass privacy legislation. A corollary inference, which is also supported by other textual evidence in section 264 and Part C of title XI, is that if Congress failed to act within the time provided, the original statutory scheme was to kick in. Under that scheme, which is set out in section 1173(e) of the House bill, the standards to be adopted were ''standards with respect to the privacy of individually identifiable health information.'' Thus, the legislative history of section 264 supports the statutory interpretation underlying the rules below.

Comment: Many commenters were opposed to the rule covering specific forms of communication or records that could potentially be considered covered information, i.e., faxes, voice mail messages, etc. A subset of these commenters took issue particularly with the inclusion of oral communications within the scope of covered information. The commenters argued that covering information when it takes oral form (e.g., verbal discussions of a submitted claim) makes the regulation extremely costly and burdensome, and even impossible to administer. Another commenter also offered that it would make it nearly impossible to discuss health information over the phone, as the covered entity cannot verify that the person on the other end is in fact who he or she claims to be.

Response: We disagree. Covering oral communications is an important part of keeping individually identifiable health information private. If the final rule were not to cover oral communication, a conversation about a person's protected health information could be shared with anyone. Therefore, the same protections afforded to paper and electronically based information must apply to verbal communication as well. Moreover, the Congress explicitly included ''oral'' information in the statutory definition of health information.

Comment: A few commenters supported, without any change, the approach proposed in the NPRM to limit the scope of covered information to individually identifiable health information in any form once the information is transmitted or maintained electronically. These commenters asserted that our statutory authority limited us accordingly. Therefore, they believed we had proposed protections to the extent possible within the bounds of our statutory authority and could not expand the scope of such protections without new legislative authority.

Response: We disagree with these commenters regarding the limitations under our statutory authority. As explained above, we have the authority to extend the scope of the regulation as we have done in the final rule. We also note here that most of these commenters who supported the NPRM's proposed approach, voiced strong support for extending the scope of coverage to all individually identifiable health information in any form, but concluded that we had done what we could within the authority provided.

Comment: One commenter argued that the term ''transaction'' is generally understood to denote a business matter, and that the NPRM applied the term too broadly by including hospital directory information, communication with a patient's family, researchers' use of data and many other non-business activities.

Response: This comment reflects a misunderstanding of our use of the term ''transaction.'' The uses and disclosures described in the comment are not ''transactions'' as defined in § 160.103. The authority to regulate the types of uses and disclosures described is provided under section 264 of Pub. L. 104–191. The conduct of the activities noted by the commenters are not related to the determination of whether a health care provider is a covered entity. We explain in the preamble that a health care provider is a covered entity if it transmits health information in electronic form in connection with transactions referred to in section 1173(a)(1) of the Act.

Comment: A few commenters asserted that the Secretary has no authority to regulate ''use'' of protected health information. They stated that although section 264(b) mentions that the Secretary should address ''uses and disclosures,'' no other section of HIPAA employs the term ''use.''

Response: We disagree with these commenters. As they themselves note, the authority to regulate use is given in section 264(b) and is sufficient.

Comment: Some commenters requested clarification as to how certain types of health information, such as photographs, faxes, X-Rays, CT-scans, and others would be classified as protected or not under the rule.

Response: All types of individually identifiable health information in any form, including those described, when maintained or transmitted by a covered entity are covered in the final rule.

Comment: A few commenters requested clarification with regard to the differences between the definitions of individually identifiable health information and protected health information.

Response: In expanding the scope of covered information in the final rule, we have simplified the distinction between the two definitions. In the final rule, protected health information is the subset of individually identifiable health information that is maintained or transmitted by covered entity, and thereby protected by this rule. For additional discussion of protected health information and individually identifiable health information, see the descriptive summary of § 164.501.

Comment: A few commenters remarked that the federal government has no right to access or control any medical records and that HHS must get consent in order to store or use any individually identifiable health information.

Response: We understand the commenters' concern. It is not our intent, nor do we through this rule create any government right of access to medical records, except as needed to investigate possible violations of the rule. Some government programs, such as Medicare, are authorized under other law to gain access to certain beneficiary records for administrative purposes. However, these programs are covered by the rule and its privacy protections apply.

Comment: Some commenters asked us to clarify how schools would be treated by the rule. Some of these commenters worried that privacy would be compromised if schools were exempted from the provisions of the final rule. Other commenters thought that school medical records were included in the provisions of the NPRM.

Response: We agree with the request for clarification and provide guidance regarding the treatment of medical records in schools in the ''Relationship to Other Federal Laws'' preamble discussion of FERPA, which governs the privacy of education records.

Comment: One commenter was concerned that only some information from a medical chart would be included as covered information. The commenter was especially concerned that transcribed material might not be considered covered information.

Response: As stated above, all individually identifiable health information in any form, including transcribed or oral information, maintained or transmitted by a covered entity is covered under the provisions of the final rule.

Comment: In response to our solicitation of comments on the scope of the definition of protected health information, many commenters asked us to narrow the scope of the proposed definition to include only information in electronic form. Others asked us to include only information from the HIPAA standard transactions.

Response: For the reasons stated by the commenters who asked us to expand the proposed definition, we reject these comments. We reject these approaches for additional reasons, as well. Limiting the protections to electronic information would, in essence, protect information only as long as it remained in a computer or other electronic media; the protections in the rule could be avoided simply by printing out the information. This approach would thus result in the illusion, but not the reality, of privacy protections. Limiting protection to information in HIPAA transactions has many of the problems in the proposed approach: it would fail to protect significant amounts of health information, would force covered entities to figure out which information had and had not been in such a transaction, and could cause the administrative burdens the commenters feared would result from protecting some but not all information.

Comment: A few commenters asserted that the definition of protected health information should explicitly include ''genetic'' information. It was argued that improper disclosure and use of such information could have a profound impact on individuals and families.

Response: We agree that the definition of protected health information includes genetic information that otherwise meets the statutory definition. But we believe that singling out specific types of protected health information for special mention in the regulation text could wrongly imply that other types are not included.

Comment: One commenter recommended that the definition of protected health information be modified to clarify that an entity does not become a 'covered entity' by providing a device to an individual on which protected health information may be stored, provided that the company itself does not store the individual's health information.''

Response: We agree with the commenter's analysis, but believe the definition is sufficiently clear without a specific amendment to this effect.

Comment: One commenter recommended that the definition be amended to explicitly exclude individually identifiable health information maintained, used, or disclosed pursuant to the Fair Credit Reporting Act, as amended, 15 U.S.C. 1681. It was stated that a disclosure of payment history to a consumer reporting agency by a covered entity should not be considered protected health information. Another commenter recommended that health information, billing information, and a consumer's credit history be exempted from the definition because this flow of information is regulated by both the Fair Credit Reporting Act (FCRA) and the Fair Debt Collection Practices Act (FDCPA).

Response: We disagree. To the extent that such information meets the definition of protected health information, it is covered by this rule. These statutes are designed to protect financial, not health, information. Further, these statutes primarily regulate entities that are not covered by this rule, minimizing the potential for overlap or conflict. The protections in this rule are more appropriate for protecting health information. However, we add provisions to the definition of payment which should address these concerns. See the definition of 'payment' in § 164.501.

Comment: An insurance company recommended that the rule require that medical records containing protected health information include a notation on a cover sheet on such records.

Response: Since we have expanded the scope of protected health information, there is no need for covered entities to distinguish among their records, and such a notation is not needed. This uniform coverage eliminates the mixed record problem and resultant potential for confusion.

Comment: A government agency requested clarification of the definition to address the status of information that flows through dictation services.

Response: A covered entity may disclose protected health information for transcription of dictation under the definition of health care operations, which allows disclosure for ''general administrative'' functions. We view transcription and clerical services generally as part of a covered entity's general administrative functions. An entity transcribing dictation on behalf of a covered entity meets this rule's definition of business associate and may receive protected health information under a business associate contract with the covered entity and subject to the other requirements of the rule.

Comment: A commenter recommended that information transmitted for employee drug testing be exempted from the definition.

Response: We disagree that is necessary to specifically exclude such information from the definition of protected health information. If a covered entity is involved, triggering this rule, the employer may obtain authorization from the individuals to be tested. Nothing in this rule prohibits an employer from requiring an employee to provide such an authorization as a condition of employment.

Comment: A few commenters addressed our proposal to exclude individually identifiable health information in education records covered by FERPA. Some expressed support for the exclusion. One commenter recommended adding another exclusion to the definition for the treatment records of students who attend institutions of post secondary education or who are 18 years old or older to avoid confusion with rules under FERPA. Another commenter suggested that the definition exclude health information of participants in ''Job Corps programs'' as it has for educational records and inmates of correctional facilities.

Response: We agree with the commenter on the potential for confusion regarding records of students who attend post-secondary schools or who are over 18, and therefore in the final rule we exclude records defined at 20 U.S.C. 1232g(a)(4)(B)(iv) from the definition of protected health information. For a detailed discussion of this change, refer to the ''Relationship to Other Federal Laws'' section of the preamble. We find no similar reason to exclude ''Job Corps programs'' from the requirements of this regulation.

Comment: Some commenters voiced support for the exclusion of the records of inmates from the definition of protected health information, maintaining that correctional agencies have a legitimate need to share some health information internally without authorization between health service units in various facilities and for purposes of custody and security. Other commenters suggested that the proposed exclusion be extended to individually identifiable health information: created by covered entities providing services to inmates or detainees under contract to such facilities; of ''former'' inmates; and of persons who are in the custody of law enforcement officials, such as the United States Marshals Service and local police agencies. They stated that

corrections and detention facilities must be able to share information with law enforcement agencies such as the United States Marshals Service, the Immigration and Naturalization Services, county jails, and U.S. Probation Offices.

Another commenter said that there is a need to have access to records of individuals in community custody and explained that these individuals are still under the control of the state or local government and the need for immediate access to records for inspections and/or drug testing is necessary.

A number of commenters were opposed to the proposed exclusion to the definition of protected health information, arguing that the proposal was too sweeping. Commenters stated that while access without consent is acceptable for some purposes, it is not acceptable in all circumstances. Some of these commenters concurred with the sharing of health care information with other medical facilities when the inmate is transferred for treatment. These commenters recommended that we delete the exception for jails and prisons and substitute specific language about what information could be disclosed and the limited circumstances or purposes for which such disclosures could occur.

Others recommended omission of the proposed exclusion entirely, arguing that excluding this information from protection sends the message that, with respect to this population, abuses do not matter. Commenters argued that inmates and detainees have a right to privacy of medical records and that individually identifiable health information obtained in these settings can be misused, e.g., when communicated indiscriminately, health information can trigger assaults on individuals with stigmatized conditions by fellow inmates or detainees. It can also lead to the denial of privileges, or inappropriately influence the deliberations of bodies such as parole boards.

A number of commenters explicitly took issue with the exclusion relative to individuals, and in particular youths, with serious mental illness, seizure disorders, and emotional or substance abuse disorders. They argued that these individuals come in contact with criminal justice authorities as a result of behaviors stemming directly from their illness and assert that these provisions will cause serious problems. They argue that disclosing the fact that an individual was treated for mental illness while incarcerated could seriously impair the individual's reintegration into the community. Commenters stated that such disclosures could put the individual or family members at risk of discrimination by employers and in the community at large.

Some commenters asserted that the rule should be amended to prohibit jails and prisons from disclosing private medical information of individuals who have been discharged from these facilities. They argued that such disclosures may seriously impair individuals' rehabilitation into society and subject them to discrimination as they attempt to re-establish acceptance in the community.

Response: We find commenters' arguments against a blanket exemption from privacy protection for inmates persuasive. We agree health information in these settings may be misused, which consequently poses many risks to the inmate or detainee and in some cases, their families as described above by the commenters. Accordingly, we delete this exception from the definition of ''protected health information'' in the final rule. The final rule considers individually identifiable health information of individuals who are prisoners and detainees to be protected health information to the extent that it meets the definition and is maintained or transmitted by a covered entity.

At the same time, we agree with those commenters who explained that correctional facilities have legitimate needs for use and sharing of individually identifiable health information inmates without authorization. Therefore, we add a new provision (§ 164.512(k)(5)) that permits a covered entity to disclose protected health information about inmates without individual consent, authorization, or agreement to correctional institutions for specified health care and other custodial purposes. For example, covered entities are permitted to disclose for the purposes of providing health care to the individual who is the inmate, or for the health and safety of other inmates or officials and employees of the facility. In addition, a covered entity may disclose protected health information as necessary for the administration and maintenance of the safety, security, and good order of the institution. See the preamble discussion of the specific requirements at § 164.512(k)(5), as well as discussion of certain limitations on the rights of individuals who are inmates with regard to their protected health information at §§ 164.506, 164.520, 164.524, and 164.528.

We also provide the following clarifications. Covered entities that provide services to inmates under contract to correctional institutions must treat protected health information about inmates in accordance with this rule and are permitted to use and disclose such information to correctional institutions as allowed under § 164.512(k)(5).

As to former inmates, the final rule considers such persons who are released on parole, probation, supervised release, or are otherwise no longer in custody, to be individuals who are not inmates. Therefore, the permissible disclosure provision at § 164.512(k)(5) does not apply in such cases. Instead, a covered entity must apply privacy protections to the protected health information about former inmates in the same manner and to the same extent that it protects the protected health information of other individuals. In addition, individuals who are former inmates hold the same rights as all other individuals under the rule.

As to individuals in community custody, the final rule considers inmates to be those individuals who are incarcerated in or otherwise confined to a correctional institution. Thus, to the extent that community custody confines an individual to a particular facility, § 164.512(k)(5) is applicable.

Psychotherapy Notes

Comment: Some commenters thought the definition of psychotherapy notes was contrary to standard practice. They claimed that reports of psychotherapy are typically part of the medical record and that psychologists are advised, for ethical reasons and liability risk management purposes, not to keep two separate sets of notes. Others acknowledged that therapists may maintain separate notations of therapy sessions for their own purpose. These commenters asked that we make clear that psychotherapy notes, at least in summary form, should be included in the medical record. Many plans and providers expressed concern that the proposed definition would encourage the creation of ''shadow'' records which may be dangerous to the patient and may increase liability for the health care providers. Some commenters claimed that psychotherapy notes contain information that is often essential to treatment.

Response: We conducted fact-finding with providers and other knowledgeable parties to determine the standard practice of psychotherapists and determined that only some psychotherapists keep separate files with notes pertaining to psychotherapy sessions. These notes are often referred to as ''process notes,'' distinguishable from ''progress notes,'' ''the medical record,'' or ''official records.'' These process notes capture the therapist's

impressions about the patient, contain details of the psychotherapy conversation considered to be inappropriate for the medical record, and are used by the provider for future sessions. We were told that process notes are often kept separate to limit access, even in an electronic record system, because they contain sensitive information relevant to no one other than the treating provider. These separate ''process notes'' are what we are calling ''psychotherapy notes.'' Summary information, such as the current state of the patient, symptoms, summary of the theme of the psychotherapy session, diagnoses, medications prescribed, side effects, and any other information necessary for treatment or payment, is always placed in the patient's medical record. Information from the medical record is routinely sent to insurers for payment.

Comment: Various associations and their constituents asked that the exceptions for psychotherapy notes be extended to health care information from other health care providers. These commenters argued that psychotherapists are not the only providers or even the most likely providers to discuss sensitive and potentially embarrassing issues, as treatment and counseling for mental health conditions, drug abuse, HIV/AIDS, and sexual problems are often provided outside of the traditional psychiatric settings. One writer stated, ''A prudent health care provider will always assess the past and present psychiatric medical history and symptoms of a patient.''

Many commenters believed that the psychotherapy notes should include frequencies of treatment, results of clinical tests, and summary of diagnosis, functional status, the treatment plan, symptoms, prognosis and progress to date. They claimed that this information is highly sensitive and should not be released without the individual's written consent, except in cases of emergency. One commenter suggested listing the types of mental health information that can be requested by third party payors to make payment determinations and defining the meaning of each term.

Response: As discussed above and in the NPRM, the rationale for providing special protection for psychotherapy notes is not only that they contain particularly sensitive information, but also that they are the personal notes of the therapist, intended to help him or her recall the therapy discussion and are of little or no use to others not involved in the therapy. Information in these notes is not intended to communicate to, or even be seen by, persons other than the therapist. Although all psychotherapy information may be considered sensitive, we have limited the definition of psychotherapy notes to only that information that is kept separate by the provider for his or her own purposes. It does not refer to the medical record and other sources of information that would normally be disclosed for treatment, payment, and health care operations.

Comment: One commenter was particularly concerned that the use of the term ''counseling'' in the definition of psychotherapy notes would lead to confusion because counseling and psychotherapy are different disciplines.

Response: In the final rule, we continue to use the term ''counseling'' in the definition of ''psychotherapy.'' During our fact-finding, we learned that ''counseling'' had no commonly agreed upon definition, but seemed to be widely understood in practice. We do not intend to limit the practice of psychotherapy to any specific professional disciplines.

Comment: One commenter noted that the public mental health system is increasingly being called upon to integrate and coordinate services among other providers of mental health services and they have developed an integrated electronic medical record system for state-operated hospitals, part of which includes psychotherapy notes, and which cannot be easily modified to provide different levels of confidentiality. Another commenter recommended allowing use or disclosure of psychotherapy notes by members of an integrated health care facility as well as the originator.

Response: The final rule makes it clear that any notes that are routinely shared with others, whether as part of the medical record or otherwise, are, by definition, not psychotherapy notes, as we have defined them. To qualify for the definition and the increased protection, the notes must be created and maintained for the use of the provider who created them i.e., the originator, and must not be the only source of any information that would be critical for the treatment of the patient or for getting payment for the treatment. The types of notes described in the comment would not meet our definition for psychotherapy notes.

Comment: Many providers expressed concern that if psychotherapy notes were maintained separately from other protected health information, other health providers involved in the individual's care would be unable to treat the patient properly. Some recommended that if the patient does not consent to sharing of psychotherapy notes for treatment purposes, the treating provider should be allowed to decline to treat the patient, providing a referral to another provider.

Response: The final rule retains the policy that psychotherapy notes be separated from the remainder of the medical record in order to receive additional protection. We based this decision on conversations with mental health providers who have told us that information that is critical to the treatment of individuals is normally maintained in the medical record and that psychotherapy notes are used by the provider who created them and rarely for other purposes. A strong part of the rationale for the special treatment of psychotherapy notes is that they are the personal notes of the treating provider and are of little or no use to others who were not present at the session to which the notes refer.

Comment: Several commenters requested that we clarify that the information contained in psychotherapy notes is being protected under the rule and not the notes themselves. They were concerned that the protection for psychotherapy notes would not be meaningful if health plans could demand the same information in a different format.

Response: This rule provides special protection for the information in psychotherapy notes, but it does not extend that protection to the same information that may be found in other locations. We do not require the notes to be in a particular format, such as hand-written. They may be typed into a word processor, for example. Copying the notes into a different format, per se, would not allow the information to be accessed by a health plan. However, the requirement that psychotherapy notes be kept separate from the medical record and solely for the use of the provider who created them means that the special protection does not apply to the same information in another location.

Public Health Authority

Comment: A number of the comments called for the elimination of all permissible disclosures without authorization, and some specifically cited the public health section and its liberal definition of public health authority as an inappropriately broad loophole that would allow unfettered access to private medical information by various government authorities.

Other commenters generally supported the provision allowing disclosure to public health authorities and to non-governmental entities

authorized by law to carry out public health activities. They further supported the broad definition of public health authority and the reliance on broad legal or regulatory authority by public health entities although explicit authorities were preferable and better informed the public.

Response: In response to comments arguing that the provision is too broad, we note that section 1178(b) of the Act, as explained in the NPRM, explicitly carves out protection for state public health laws. This provision states that: ''[N]othing in this part shall be construed to invalidate or limit the authority, power, or procedures established under any law providing for the reporting of disease or injury, child abuse, birth or death, public health surveillance, or public health investigation or intervention.'' In light of this broad Congressional mandate not to interfere with current public health practices, we believe the broad definition of ''public health authority'' is appropriate to achieve that end.

Comment: Some commenters said that they performed public health activities in analyzing data and information. These comments suggested that activities conducted by provider and health plan organizations that compile and compare data for benchmarking performance, monitoring, utilization, and determining the health needs of a given market should be included as part of the public health exemption. One commenter recommended amending the regulation to permit covered entities to disclose protected health information to private organizations for public health reasons.

Response: We disagree that such a change should be made. In the absence of some nexus to a government public health authority or other underlying legal authority, covered entities would have no basis for determining which data collections are ''legitimate'' and how the confidentiality of the information will be protected. In addition, the public health functions carved out for special protection by Congress are explicitly limited to those established by law.

Comment: Two commenters asked for additional clarification as to whether the Occupational Safety and Health Administration (OSHA) and the Mine Safety and Health Administration (MSHA) would be considered public health authorities as indicated in the preamble. They suggested specific language for the final rule. Commenters also suggested that we specify that states operating OSHA-approved programs also are considered public health authorities. One comment applauded the Secretary's recognition of OSHA as both a health oversight agency and public health authority. It suggested adding OSHA-approved programs that operate in states to the list of entities included in these categories. In addition, the comment requested the final regulation specifically mention these entities in the text of the regulation as well.

Response: We agree that OSHA, MSHA and their state equivalents are public health authorities when carrying out their activities related to the health and safety of workers. We do not specifically reference any agencies in the regulatory definition, because the definition of public health authority and this preamble sufficiently address this issue. As defined in the final rule, the definition of ''public health authority'' at § 164.501 continues to include OSHA as a public health authority. State agencies or authorities responsible for public health matters as part of their official mandate, such as OSHA-approved programs, also come within this definition. See discussion of § 164.512(b) below. We have refrained, however, from listing specific agencies and have retained a general descriptive definition.

Comments: Several commenters recommended expanding the definition of public health authority to encompass other governmental entities that may collect and hold health data as part of their official duties. One recommended changing the definition of public health authority to read as follows: Public health authority means an agency or authority * * * that is responsible for public health matters or the collection of health data as part of its official mandate.

Response: We do not adopt this recommendation. The public health provision is not intended to cover agencies that are not responsible for public health matters but that may in the course of their responsibilities collect health-related information. Disclosures to such authorities may be permissible under other provision of this rule.

Comment: Many commenters asked us to include a formal definition of ''required by law'' incorporating the material noted in this preamble and additional suggested disclosures.

Response: We agree generally and modify the definition accordingly. See discussion above.

Research

Comment: We received many comments from supporting the proposed definition of ''research.'' These commenters agreed that the definition of ''research'' should be the same as the definition in the Common Rule. These commenters argued that it was important that the definition of ''research'' be consistent with the Common Rule's definition to ensure the coherent oversight of medical research. In addition, some of these commenters also supported this definition because they believed it was already well-understood by researchers and provided reasonably clear guidance needed to distinguish between research and health care operations.

Some commenters, believed that the NPRM's definition was too narrow. Several of these commenters agreed that the Common Rule's definition should be adopted in the final rule, but argued that the proposed definition of ''generalizable knowledge'' within the definition of ''research,'' which limited generalizable knowledge to knowledge that is ''related to health,'' was too narrow. For example, one commenter stated that gun shot wound, spousal abuse, and other kinds of information from emergency room statistics are often used to conduct research with ramifications for social policy, but may not be ''related to health.'' Several of these commenters recommended that the definition of research be revised to delete the words ''related to health.'' Additional commenters who argued that the definition was too narrow raised the following concerns: the difference between ''research'' and ''health care operations'' is irrelevant from the patients' perspective, and therefore, the proposed rule should have required documentation of approval by an IRB or privacy board before protected health information could be used or disclosed for either of these purposes, and the proposed definition was too limited because it did not capture research conducted by non-profit entities to ensure public health goals, such as disease-specific registries.

Commenters who argued that the definition was too broad recommended that certain activities should be explicitly excluded from the definition. In general, these commenters were concerned that if certain activities were considered to be ''research'' the rule's research requirements would represent a problematic level of regulation on industry initiatives. Some activities that these commenters recommended be explicitly excluded from the definition of ''research'' included: marketing research, health and productivity management, quality assessment and improvement activities, and internal research conducted to improve health.

Response: We agree that the final rule's definition of ''research'' should be

consistent with the Common Rule's definition of this term. We also agree that our proposal to limit ''generalizable knowledge'' to knowledge that is ''related to health,'' and ''knowledge that could be applied to populations outside of the population served by the covered entity,'' was too narrow. Therefore, in the final rule, we retain the Common Rule's definition of ''research'' and eliminate the further elaboration of ''generalizable knowledge.'' We understand knowledge to be generalizable when it can be applied to either a population inside or outside of the population served by the covered entity. Therefore, knowledge may be ''generalizable'' even if a research study uses only the protected health information held within a covered entity, and the results are generalizable only to the population served by the covered entity. For example, generalizable knowledge could be generated from a study conducted by the HCFA, using only Medicare data held by HCFA, even if the knowledge gained from the research study is applicable only to Medicare beneficiaries.

We rejected the other arguments claiming that the definition of ''research'' was either too narrow or too broad. While we agree that it is sometimes difficult to distinguish between ''research'' and ''health care operations,'' we disagree that the difference between these activities is irrelevant from the patients' perspective. We believe, based on many of the comments, that individuals expect that individually identifiable health information about themselves will be used for health care operations such as reviewing the competence or qualifications of health care professionals, evaluating provider and plan performance, and improving the quality of care. A large number of commenters, however, indicated that they did not expect that individually identifiable health information about themselves would be used for research purposes without their authorization. Therefore, we retain more stringent protections for research disclosures without patient authorization.

We also disagree with the commenters who were concerned that the proposed definition was too limited because it did not capture research conducted by non-profit entities to ensure public health goals, such as disease-specific registries. Such activities conducted by either non-profit or for-profit entities could meet the rule's definition of research, and therefore are not necessarily excluded from this definition.

We also disagree with many of the commenters who argued that certain activities should be explicitly excluded from the definition of research. We found no persuasive evidence that, when particular activities are also systematic investigations designed to contribute to generalizable knowledge, they should be treated any different from other such activities.

We are aware that the National Bioethics Advisory Commission (NBAC) is currently assessing the Common Rule's definition of ''research'' as part of a report they are developing on the implementation and adequacy of the Common Rule. Since we agree that a consistent definition is important to the conduct and oversight of research, if the Common Rule's definition of ''research'' is modified in the future, the Department of Health and Human Services will consider whether the definition should also be modified for this subpart.

Comment: Some commenters urged the Department to establish precise definitions for ''health care operations'' and ''research'' to provide clear guidance to covered entities and adequate privacy protections for the subjects of the information whose information is disclosed for these purposes. One commenter supported the definition of ''research'' proposed in the NPRM, but was concerned about the ''crossover'' from data analyses that begin as health care operations but later become ''research'' because the analytical results are of such importance that they should be shared through publication, thereby contributing to generalizable knowledge. To distinguish between the definitions of ''health care operations'' and ''research,'' a few commenters recommended that the rule make this distinction based upon whether the activity is a ''use'' or a ''disclosure.'' These commenters recommend that the ''use'' of protected health information for research without patient authorization should be exempt from the proposed research provisions provided that protected health information was not disclosed in the final analysis, report, or publication.

Response: We agree with commenters that at times it may be difficult to distinguish projects that are health operations and projects that are research. We note that this ambiguity exists today, and disagree that we can address this issue with more precise definitions of research and health care operations. Today, the issue is largely one of intent. Under the Common Rule, the ethical and regulatory obligations of the researcher stem from the intent of the activity. We follow that approach here. If such a project is a systematic investigation that designed to develop or contribute to generalizable knowledge, it is considered to be ''research,'' not ''health care operations.''

In some instances, the primary purpose of the activity may change as preliminary results are analyzed. An activity that was initiated as an internal outcomes evaluation may produce information that could be generalized. If the purpose of a study changes and the covered entity does intend to generalize the results, the covered entity should document the fact as evidence that the activity was not subject to § 164.512(i) of this rule.

We understand that for research that is subject to the Common Rule, this is not the case. The Office for Human Research Protection interprets 45 CFR part 46 to require IRB review as soon as an activity meets the definition of research, regardless of whether the activity began as ''health care operations'' or ''public health,'' for example. The final rule does not affect the Office of Human Research Protection's interpretation of the Common Rule.

We were not persuaded that an individual's privacy interest is of less concern when covered entities use protected health information for research purposes than when covered entities disclose protected health information for research purposes. We do not agree generally that internal activities of covered entities do not potentially compromise the privacy interests of individuals. Many persons within a covered entity may have access to protected health information. When the activity is a systematic investigation, the number of persons who may be involved in the records review and analysis may be substantial. We believe that IRB or privacy board approval of the waiver of authorization will provide important privacy protections to individuals about whom protected health information is used or disclosed for research. If a covered entity wishes to use protected health information about its enrollees for research purposes, documentation of an IRBs' or privacy board's assessment of the privacy impact of such a use is as important as if the same research study required the disclosure of protected health information. This conclusion is consistent with the Common Rule's requirement for IRB review of all human subjects research.

Treatment

Comment: Some commenters advocated for a narrow interpretation of

treatment that applies only to the individual who is the subject of the information. Other commenters asserted that treatment should be broadly defined when activities are conducted by health care providers to improve or maintain the health of the patient. A broad interpretation may raise concerns about potential misuse of information, but too limited an interpretation will limit beneficial activities and further contribute to problems in patient compliance and medical errors.

Response: We find the commenters' arguments for a broad definition of treatment persuasive. Today, health care providers consult with one another, share information about their experience with particular therapies, seek advice about how to handle unique or challenging cases, and engage in a variety of other discussions that help them maintain and improve the quality of care they provide. Quality of care improves when providers exchange information about treatment successes and failures. These activities require sharing of protected health information. We do not intend this rule to interfere with these important activities. We therefore define treatment broadly and allow use and disclosure of protected health information about one individual for the treatment of another individual.

Under this definition, only health care providers or a health care provider working with a third party can perform treatment activities. In this way, we temper the breadth of the definition by limiting the scope of information sharing. The various codes of professional ethics also help assure that information sharing among providers for treatment purposes will be appropriate.

We note that poison control centers are health care providers for purposes of this rule. We consider the counseling and follow-up consultations provided by poison control centers with individual providers regarding patient outcomes to be treatment. Therefore, poison control centers and other health care providers can share protected health information about the treatment of an individual without a business associate contract.

Comment: Many commenters suggested that ''treatment'' activities should include services provided to both a specific individual and larger patient populations and therefore urged that the definition of treatment specifically allow for such activities, sometimes referred to as ''disease management'' activities. Some argued that an analysis of an overall population is integral to determining which individuals would benefit from disease management services. Thus, an analysis of health care claims for enrolled populations enables proactive contact with those identified individuals to notify them of the availability of services. Certain commenters noted that ''disease management'' services provided to their patient populations, such as reminders about recommended tests based on nationally accepted clinical guidelines, are integral components of quality health care.

Response: We do not agree that population based services should be considered treatment activities. The definition of ''treatment'' is closely linked to the § 160.103 definition of ''health care,'' which describes care, services and procedures related to the health of an individual. The activities described by ''treatment,'' therefore, all involve health care providers supplying health care to a particular patient. While many activities beneficial to patients are offered to entire populations or involve examining health information about entire populations, treatment involves health services provided by a health care provider and tailored to the specific needs of an individual patient. Although a population-wide analysis or intervention may prompt a health care provider to offer specific treatment to an individual, we consider the population-based analyses to improve health care or reduce health care costs to be health care operations (see definition of ''health care operations,'' above).

Comment: A number of commenters requested clarification about whether prescription drug compliance management programs would be considered ''treatment.'' One commenter urged HHS to clarify that provision by a pharmacy to a patient of customized prescription drug information about the risks, benefits, and conditions of use of a prescription drug being dispensed is considered a treatment activity. Others asked that the final rule expressly recognize that prescription drug advice provided by a dispensing pharmacist, such as a customized pharmacy letter, is within the scope of treatment.

Response: The activities that are part of prescription drug compliance management programs were not fully described by these commenters, so we cannot state a general rule regarding whether such activities constitute treatment. We agree that pharmacists' provision of customized prescription drug information and advice about the prescription drug being dispensed is a treatment activity. Pharmacists' provisions of information and counseling about pharmaceuticals to their customers constitute treatment, and we exclude certain communications made in the treatment context from the definition of marketing. (See discussion above.)

Comment: Some commenters noted the issues and recommendations raised in the Institutes of Medicine report ''To Err Is Human'' and the critical need to share information about adverse drug and other medical events, evaluation of the information, and its use to prevent future medical errors. They noted that privacy rules should not be so stringent as to prohibit the sharing of patient data needed to reduce errors and optimize health care outcomes. To bolster the notion that other programs associated with the practice of pharmacy must be considered as integral to the definition of health care and treatment, they reference OBRA '90 (42 U.S.C. 1396r–8) and the minimum required activities for dispensing drugs; they also note that virtually every state Board of Pharmacy adopted regulations imposing OBRA'90 requirements on pharmacies for all patients and not just Medicaid recipients.

Response: We agree that reducing medical errors is critical, and do not believe that this regulation impairs efforts to reduce medical errors. We define treatment broadly and include quality assessment and improvement activities in the definition of health care operations. Covered pharmacies may conduct such activities, as well as treatment activities appropriate to improve quality and reduce errors. We believe that respect for the privacy rights of individuals and appropriate protection of the confidentiality of their health information are compatible with the goal of reducing medical errors.

Comment: Some commenters urged us to clarify that health plans do not perform ''treatment'' activities; some of these were concerned that a different approach in this regulation could cause conflict with state corporate practice of medicine restrictions. Some commenters believed that the proposed definition of treatment crossed into the area of cost containment, which would seem to pertain more directly to payment. They supported a narrower definition that would eliminate any references to third party payors. One commenter argued that the permissible disclosure of protected health information to carry out treatment is too broad for health plans and that health plans that have no responsibility for treatment or care coordination should have no authority to release health information without authorization for treatment purposes.

Response: We do not consider the activities of third party payors, including health plans, to be

''treatment.'' Only health care providers, not health plans, conduct ''treatment'' for purposes of this rule. A health plan may, however, disclose protected health information without consent or authorization for treatment purposes if that disclosure is made to a provider. Health plans may have information the provider needs, for example information from other providers or information about the patient's treatment history, to develop an appropriate plan of care.

Comment: We received many comments relating to ''disease management'' programs and whether activities described as disease management should be included in the definition of treatment. One group of commenters supported the proposed definition of treatment that includes disease management. One commenter offered the position that disease management services are more closely aligned with treatment because they involve the coordination of treatment whereas health care operations are more akin to financial and ministerial functions of plans.

Some recommended that the definition of treatment be limited to direct treatment of individual patients and not allow for sharing of information for administrative or other programmatic reasons. They believed that allowing disclosures for disease management opens a loophole for certain uses and disclosures, such as marketing, that should only be permitted with authorization. Others recommended that the definition of disease management be restricted to prevent unauthorized use of individual health records to target individuals in a health plan or occupational health program. Many asked that the definition of disease management be clarified to identify those functions that, although some might consider them to be subsumed by the term, are not permitted under this regulation without authorization, such as marketing and disclosures of protected health information to employers. They suggested that disease management may describe desirable activities, but is subject to abuse and therefore should be restricted and controlled. One commenter recommends that we adopt a portion of the definition adopted by the Disease Management Association of America in October 1999.

On the other hand, many comments urged that disease management be part of the ''treatment'' definition or the ''health care operations'' definition and asked that specific activities be included in a description of the term. They viewed disease management as important element of comprehensive health care services and cost management efforts. They recommended that the definition of disease management include services directed at an entire population and not just individual care, in order to identify individuals who would benefit from services based on accepted clinical guidelines. They recommended that disease management be included under health care operations and include population level services. A commenter asserted that limiting disease management programs to the definition of treatment ignores that these programs extend beyond providers, especially since NCQA accreditation standards strongly encourage plans and insurers to provide these services.

Response: Disease management appeared to represent different activities to different commenters. Our review of the literature, industry materials, state and federal statutes,[6] and discussions with physician groups, health plan groups and disease management associations confirm that a consensus definition from the field has not yet evolved, although efforts are underway. Therefore, rather than rely on this label, we delete ''disease management'' from the treatment definition and instead include the functions often discussed as disease management activities in this definition or in the definition of health care operations and modify both definitions to address the commenters' concerns.

We add population-based activities to improve health care or reduce health care costs to the definition of health care operations. Outreach programs as described by the commenter may be considered either health care operations or treatment, depending on whether population-wide or patient-specific activities occur, and if patient-specific, whether the individualized communication with a patient occurs on behalf of health care provider or a health plan. For example, a call placed by a nurse in a doctor's office to a patient to discuss follow-up care is a treatment activity. The same activity performed by a nurse working for a health plan would be a health care operation. In both cases, the database analysis that created a list of patients that would benefit from the intervention would be a health care operation. Use or disclosure of protected health information to provide education materials to patients may similarly be either treatment or operations, depending on the circumstances and on who is sending the materials. We cannot say in the abstract whether any such activities constitute marketing under this rule. See §§ 164.501 and 164.514 for details on what communications are marketing and when the authorization of the individual may be required.

Comment: Many commenters were concerned that the definition of treatment would not permit Third Party Administrators (TPAs) to be involved with disease management programs without obtaining authorization. They asserted that while the proposed definition of treatment included disease management conducted by health care providers it did not recognize the role of employers and TPAs in the current disease management process.

Response: Covered entities disclose protected health information to other persons, including TPAs, that they hire to perform services for them or on their behalf. If a covered entity hires a TPA to perform the disease management activities included in the rule's definitions of treatment and health care operations that disclosure will not

[6] Definition of Disease Management, October 1999 (from web site of Disease Management Association of America (www.dmaa.org/definition.html) accessed May 21, 2000. Other references used for our analysis include: Mary C. Gurnee, et al, Constructing Disease Management Programs, Managed Care, June 1997, accessed at http://managedcaremag.com, 5/19/2000; Peter Wehrwein, Disease Management Gains a Degree of Respectability, Managed Care, August 1997, accessed at www.managedcaremag.com, 5/18/00; John M. Harris, Jr., disease management: New Wine in Old Bottles, 124 Annals of Internal Medicine 838 (1996); Robert S. Epstein and Louis M. Sherwood, From Outcomes research to disease management: A Guide for the Perplexed, 124 Annals of Internal Medicine 832 (1996); Anne Mason et al, disease management, the Pharmaceutical Industry and the NHS, Office of Health Economics (United Kingdom), accessed at www.ohe.org, 5/19/2000; Thomas Bodenheimer, Disease Management—Promises and Pitfalls, 340 New Eng. J. Med, April 15, 1999, accessed at www.nejm.org, 4/20/99; Bernard Lo and Ann Alpers, Uses and Abuses of Prescription Drug information in pharmacy benefits Management Programs, 283 JAMA 801 (2000); Robert F. DeBusk, Correspondence, Disease Management, and Regina E. Herzlinger, Correspondence, Disease Management, 341 New Eng. J. Med, Sept 2, 1999, accessed 9/2/99; Letter, John A. Gans, American Pharmaceutical Association, to Health Care Financing Administration, Reference HCFA–3002–P, April 12, 1999, accessed at www.aphanet.org, 1/18/2000; Ronald M. Davis, et al, Editorial, Advances in Managing Chronic Disease, 320 BMJ 525 (2000), accessed at www.bmj.com, 2/25/00; Thomas Bodenheimer, Education and Debate, disease management in the American Market, 320 BMJ 563 (2000), accessed at www.bmj.com, 2/25/2000; David J. Hunter, disease management: has it a future?, 320 BMJ 530 (2000), accessed www.bmj.com 2/25/2000; Trisha Greenhalgh, Commercial partnerships in chronic disease management: proceeding with caution, 320 BMJ 566 (2000); Edmund X. DeJesus, disease management in a Warehouse, Healthcare Informatics, September 1999, accessed at www.healthcare-informatics.com, 5/19/00; Regulation, 42 CFR 422.112, Medicare+Choice Program, subpart C, Benefits and Beneficiary Protections, sec. 422.112, Access to Services; and Arnold Chen, Best Practices in Coordinated Care, Submitted by Mathematica Policy Research, Inc., to Health Care Financing Administration, March 22, 2000.

require authorization. The relationship between the covered entity and the TPA may be subject to the business associate requirements of §§ 164.502 and 164.504. Disclosures by covered entities to plan sponsors, including employers, for the purpose of plan administration are addressed in § 164.504.

Comment: Commenters suggested that as disease management is defined only as an element of treatment, it could only be carried out by health care providers, and not health plans. They opposed this approach because health plans also conduct such programs, and are indeed required to do it by accreditation standards and HCFA Managed Care Organization standards.

Response: We agree that the placement of disease management in the proposed definition of treatment suggested that health plans could not conduct such programs. We revise the final rule to clarify that health plans may conduct population based care management programs as a health care operation activity.

Comment: Some commenters stated that the rule should require that disease management only be done with the approval of the treating physician or at least with the knowledge of the physician.

Response: We disagree with this comment because we do not believe that this privacy rule is an appropriate venue for setting policies regarding the management of health care costs or treatment.

Comment: Some industry groups stated that if an activity involves selling products, it is not disease management. They asked for a definition that differentiates use of information for the best interests of patient from uses undertaken for ''ulterior purposes'' such as advertising, marketing, or promoting separate products.

Response: We eliminate the definition of ''disease management'' from the rule. Often however, treatment decisions involve discussing the relevant advantages and disadvantages of products and services. Health plans, as part of payment and operations, sometimes communicate with individuals about particular products and services. We address these distinctions in the definitions of marketing and ''health care operations'' in § 164.501, and in the requirements for use and disclosure of protected health information for marketing in § 164.514.

Comment: Some health care providers noted that there is a danger that employers will ''force'' individual employees with targeted conditions into self-care or compliance programs in ways that violate both the employee's privacy interest and his or her right to control own medical care.

Response: Employers are not covered entities under HIPAA, so we cannot prohibit them under this rule from undertaking these or other activities with respect to health information. In § 164.504 we limit disclosure of health information from group health plans to the employers sponsoring the plans. However, other federal and/or state laws, such as disability nondiscrimination laws, may govern the rights of employees under such circumstances.

Comment: Many commenters urged that disease management only be allowed with the written consent of the individual. Others also desired consent but suggested that an opt-out would be sufficient. Other commenters complained that the absence of a definition for disease management created uncertainty in view of the proposed rule's requirement to get authorization for marketing. They were concerned that the effect would be to require patient consent for many activities that are desirable, not practicably done if authorization is required, and otherwise classifiable as treatment, payment, or health care operations. Examples provided include reminders for appointments, reminders to get preventive services like mammograms, and information about home management of chronic illnesses.

Response: We agree with the commenters who stated that the requirement for specific authorization for certain activities considered part of disease management could impede the ability of health plans and covered providers to implement effective health care management and cost containment programs. In addition, this approach would require us to distinguish activities undertaken as part of a formal disease management program from the same activities undertaken outside the context of disease management program. For example, we see no clear benefit to privacy in requiring written authorization before a physician may call a patient to discuss treatment options in all cases, nor do we see a sound basis for requiring it only when the physician was following a formal protocol as part of a population based intervention. We also are not persuaded that the risk to privacy for these activities warrants a higher degree of protection than do other payment, health care operations or treatment activities for which specific authorization was not suggested by commenters.

Comment: A few commenters asked that we clarify that disclosure of protected health information about a prospective patient to a health care provider (e.g., a possible admission to an assisted living facility from a nursing facility) is a treatment activity that does not require authorization.

Response: We agree that the described activity is ''treatment,'' because it constitutes referral and coordination of health care.

Comment: Comments called for the removal of ''other services'' from the definition.

Response: We disagree with the concept that only health care services are appropriately included in the treatment definition. We have modified this definition to instead include ''the provision, coordination, or management of health care and related services.'' This definition allows health care providers to offer or coordinate social, rehabilitative, or other services that are associated with the provision of health care. Our use of the term ''related'' prevents ''treatment'' from applying to the provision of services unrelated to health care.

Comment: Several commenters stated that the definition of treatment should include organ and tissue recovery activities. They asserted that the information exchanged and collected to request consent, evaluate medical information about a potential donor and perform organ recoveries relates to treatment and are not administrative activities. When hospitals place a patient on the UNOS list it is transferring individually identifiable health information. Also, when an organ procurement organization registers a donor with UNOS it could be disclosing protected health information. Commenters questioned whether these activities would be administrative or constitute treatment.

Response: In the proposed rule we included in the definition of ''health care'' activities related to the procurement or organs, blood, eyes and other tissues. This final rule deletes those activities from the definition of ''health care.'' We do so because, while organ and tissue procurement organizations are integral components of the health care system, we do not believe that the testing, procurement, and other procedures they undertake describe ''health care'' offered to the donors of the tissues or organs themselves. See the discussion under the definition of ''health care'' in § 160.103.

Comment: Some commenters recommended including health promotion activities in the definition of health care.

Response: We consider health promotion activities to be preventive care, and thus within the definition of health care. In addition, such activities that are population based are included in the definition of health care operations.

Comment: We received a range of comments regarding the proper placement of case and disease management in the definitions and the perceived overlap between health care operations and treatment. Some consider that these activities are a function of improving quality and controlling costs. Thus, they recommend that the Secretary move risk assessment, case and disease management to the definition of health care operations.

Response: In response to these comments, we remove these terms from the definition of treatment and add case management to the definition of health care operations. We explain our treatment of disease management in responses to comments above. Whether an activity described as disease or case management falls under treatment or health care operations would depend in part on whether the activity is focused on a particular individual or a population. A single program described as a ''case management'' effort may include both health care operations activities (e.g., records analysis, protocol development, general risk assessment) and treatment activities (e.g., particular services provided to or coordinated for an individual, even if applying a standardized treatment protocol).

Comment: We received comments that argued for the inclusion of ''disability management'' in the treatment definition. They explained that through disability management, health care providers refer and coordinate medical management and they require contemporaneous exchange of an employee's specific medical data for the provider to properly manage.

Response: To the extent that a covered provider is coordinating health care services, the provider is providing treatment. We do not include the term ''disability management'' because the scope of the activities covered by that term is not clear. In addition, the commenters did not provide enough information for us to make a fact-based determination of how this rule applies to the uses and disclosures of protected health information that are made in a particular ''disability management'' program.

Use

Comment: One commenter asserted that the scope of the proposal had gone beyond the intent of Congress in addressing uses of information within the covered entity, as opposed to transactions and disclosures outside the covered entity. This commenter argued that, although HIPAA mentions use, it is unclear that the word ''use'' in the proposed rule is what Congress intended. The commenter pointed to the legislative history to argue that ''use'' is related to an information exchange outside of the entity.

Response: We disagree with the commenter regarding the Congress' intent. Section 264 of HIPAA requires that the Secretary develop and send to Congress recommendations on standards with respect to the privacy of individually identifiable health information (which she did on September 11, 1997) and prescribes that the recommendations address among other items ''the uses and disclosures of such information that should be authorized or required.'' Section 264 explicitly requires the Secretary to promulgate standards that address at least the subjects described in these recommendations. It is therefore our interpretation that Congress intended to cover ''uses'' as well as disclosures of individually identifiable health information. We find nothing in the legislative history to indicate that Congress intended to deviate from the common meaning of the term ''use.''

Comment: One commenter observed that the definition could encompass the processing of data by computers to execute queries. It was argued that this would be highly problematic because computers are routinely used to identify subsets of data sets. It was explained that in performing this function, computers examine each record in the data set and return only those records in the data set that meet specific criteria. Consequently, a human being will see only the subset of data that the computer returns. Thus, the commenter stated that it is only this subset that could be used or disclosed.

Response: We interpret ''use'' to mean only the uses of the product of the computer processing, not the internal computer processing that generates the product.

Comments: Some commenters asked that the Department clarify that individualized medical information obtained through a fitness for duty examination is not subject to the privacy protections under the regulation.

Response: As discussed above, we have clarified that the definition of ''treatment'' to include assessments of an individual. If the assessment is performed by a covered health care provider, the health information resulting from the assessment is protected health information. We note that a covered entity is permitted to condition the provision of health care when the sole purpose is to create protected health information for the benefit of a third person. See § 164.508(b). For example, a covered health care provider may condition the provision of a fitness for duty examination to an individual on obtaining an authorization from the individual for disclosure to the employer who has requested the examination.

Section 164.502—Uses and Disclosures of Protected Health Information: General Rules

Section 164.502(a)—General Standard

Comment: A few commenters requested an exemption from the rule for the Social Security and Supplemental Security Income Disability Programs so that disability claimants can be served in a fair and timely manner. The commenters were concerned that the proposal would be narrowly interpreted, thereby impeding the release of medical records for the purposes of Social Security disability programs.

Another commenter similarly asked that a special provision be added to the proposal's general rule for uses and disclosures without authorization for treatment, payment, and health care operations purposes to authorize disclosure of all medical information from all sources to the Social Security Administration, including their contracted state agencies handling disability determinations.

Response: A complete exemption for disclosures for these programs is not necessary. Under current practice, the Social Security Administration obtains authorization from applicants for providers to release an individual's records to SSA for disability and other determinations. Thus, there is no reason to believe that an exemption from the authorization required by this rule is needed to allow these programs to function effectively. Further, such an exemption would reduce privacy protections from current levels. When this rule goes into effect, those authorizations will need to meet the requirements for authorization under § 164.508 of this rule.

We do, however, modify other provisions of the proposed rule to accommodate the special requirements of these programs. In particular, Social Security Disability and other federal programs, and public benefits programs run by the states, are authorized by law

to share information for eligibility purposes. Where another public body has determined that the appropriate balance between need for efficient administration of public programs and public funds and individuals' privacy interests is to allow information sharing for these limited purposes, we do not upset that determination. Where the sharing of enrollment and eligibility information is required or expressly authorized by law, this rule permits such sharing of information for eligibility and enrollment purposes (see § 164.512(k)(6)(i)), and also excepts these arrangements from the requirements for business associate agreements (see § 164.502(e)(1)).

Comment: A few commenters asked that the rule be revised to authorize disclosures to clergy, for directory purposes, to organ and tissue procurement organizations, and to the American Red Cross without patient authorization.

Response: We agree and revise the final rule accordingly. The new policies and the rationale for these policies are found in §§ 164.510 and 164.512, and the corresponding preamble.

Comment: One commenter recommended that the rule apply only to the ''disclosure'' of protected health information by covered entities, rather than to both ''use'' and ''disclosure.'' The commenter stated that the application of the regulation to a covered entity's use of individually identifiable health information offers little benefit in terms of protecting protected health information, yet imposes costs and may hamper many legitimate activities, that fall outside the definition of treatment, payment or health care operations.

Another commenter similarly urged that the final regulation draw substantive distinctions between restrictions on the ''use'' of individually identifiable health information and on the ''disclosure'' of such information, with broader latitude for ''uses'' of such information. The commenter believed that internal ''uses'' of such information generally do not raise the same issues and concerns that a disclosure of that information might raise. It was argued that any concerns about the potential breadth of use of this information could be addressed through application of the ''minimum necessary'' standard. The commenter also argued that Congressional intent was that a ''disclosure'' of individually identifiable health information is potentially much more significant than a ''use'' of that information.

Response: We do not accept the commenter's broad recommendation to apply the regulation only to the ''disclosure'' of protected health information and not to ''use'' of such information. Section 264 charges the Secretary with promulgating standards that address, among other things, ''the uses and disclosures'' of individually identifiable health information. We also do not agree that applying the regulation to ''use'' offers little benefit to protecting protected health information. The potential exists for misuse of protected health information within entities. This potential is even greater when the covered entity also provides services or products outside its role as a health care provider, health plan, or health care clearinghouse for which ''use'' of protected health information offers economic benefit to the entity. For example, if this rule did not limit ''uses'' generally to treatment, payment and health care operations, a covered entity that also offered financial services could be able to use protected health information without authorization to market or make coverage or rate decisions for its financial services products. Without the minimum necessary standard for uses, a hospital would not be constrained from allowing their appointment scheduling clerks free access to medical records.

We agree, however, that it is appropriate to apply somewhat different requirements to uses and disclosures of protected health information permitted by this rule. We therefore modify the application of the minimum necessary standard to accomplish this. See the preamble to § 164.514 for a discussion of these changes.

Comment: A commenter argued that the development, implementation, and use of integrated computer-based patient medical record systems, which requires efficient information sharing, will likely be impeded by regulatory restrictions on the ''use'' of protected health information and by the minimum necessary standard.

Response: We have modified the proposed approach to regulating ''uses'' of protected health information within an entity, and believe our policy is compatible with the development and implementation of computer-based medical record systems. In fact, we drew part of the revised policy on ''minimum necessary'' use of protected health information from the role-based access approach used in several computer-based records systems today. These policies are described further in § 164.514.

Comment: One commenter asked that the general rules for uses and disclosures be amended to permit covered entities to disclose protected health information for purposes relating to property and casualty benefits. The commenter argued that the proposal could affect its ability to obtain protected health information from covered entities, thereby constricting the flow of medical information needed to administer property and casualty benefits, particularly in the workers' compensation context. It was stated that this could seriously impede property and casualty benefit providers' ability to conduct business in accordance with state law.

Response: We disagree that the rule should be expanded to permit all uses and disclosures that relate to property and casualty benefits. Such a broad provision is not in keeping with protecting the privacy of individuals. Although we generally lack the authority under HIPAA to regulate the practices of this industry, the final rule addresses when covered entities may disclose protected health information to property and casualty insures. We believe that the final rule permits property and casualty insurers to obtain the protected health information that they need to maintain their promises to their policyholders. For example, the rule permits a covered entity to use or disclose protected health information relating to an individual when authorized by the individual. Property and casualty insurers are free to obtain authorizations from individuals for release by covered entities of the health information that the insurers need to administer claims, and this rule does not affect their ability to condition payment on obtaining such an authorization from insured individuals. Property and casualty insurers providing payment on a third-party basis have an opportunity to obtain authorization from the individual and to condition payment on obtaining such authorization. The final rule also permits covered entities to make disclosures to obtain payment, whether from a health plan or from another person such as a property and casualty insurer. For example, where an automobile insurer is paying for medical benefits on a first-party basis, a health care provider may disclose protected health information to the insurer as part of a request for payment. We also include in the final rule a new provision that permits covered entities to use or disclose protected health information as authorized by workers' compensation or similar programs established by law addressing work-related injuries or illness. See § 164.512(l). These statutory programs establish channels of information sharing that are necessary

to permit compensation of injured workers.

Comment: A few commenters suggested that the Department specify ''prohibited'' uses and disclosures rather than ''permitted'' uses and disclosures.

Response: We reject these commenters' because we believe that the best privacy protection in most instances is to require the individual's authorization for use or disclosure of information, and that the role of this rule is to specify those uses and disclosures for which the balance between the individuals' privacy interest and the public's interests dictates a different approach. The opposite approach would require us to anticipate the much larger set of all possible uses of information that do not implicate the public's interest, rather than to specify the public interests that merit regulatory protection.

Comment: A commenter recommended that the rule be revised to more strongly discourage the use of individually identifiable health information where de-identified information could be used.

Response: We agree that the use of de-identified information wherever possible is good privacy practice. We believe that by requiring covered entities to implement these privacy restrictions only with respect to individually identifiable health information, the final rule strongly encourages covered entities to use de-identified information as much as practicable.

Comment: One commenter recommended that when information from health records is provided to authorized external users, this information should be accompanied by a statement prohibiting use of the information for other than the stated purpose; prohibiting disclosure by the recipient to any other party without written authorization from the patient, or the patient's legal representative, unless such information is urgently needed for the patient's continuing care or otherwise required by law; and requiring destruction of the information after the stated need has been fulfilled.

Response: We agree that restricting other uses or re-disclosure of protected health information by a third party that may receive the information for treatment, payment, and health care operations purposes or other purposes permitted by rule would be ideal with regard to privacy protection. However, as described elsewhere in this preamble, once protected health information leaves a covered entity the Department no longer has jurisdiction under the statute to apply protections to the information. Since we would have no enforcement authority, the costs and burdens of requiring covered entities to produce and distribute such a statement to all recipients of protected heath information, including those with whom the covered entity has no on-going relationship, would outweigh any benefits to be gained from such a policy. Similarly, where protected health information is disclosed for routine treatment, payment and operations purposes, the sheer volume of these disclosures makes the burden of providing such a statement unacceptable. Appropriate protection for these disclosures requires law or regulation directly applicable to the recipient of the information, not further burden on the disclosing entity. Where, however, the recipient of protected health information is providing a service to or on behalf of the covered entity this balance changes. It is consistent with long-standing legal principles to hold the covered entity to a higher degree of responsibility for the actions of its agents and contractors. See § 164.504 for a discussion of the responsibilities of covered entities for the actions of their business associates with respect to protected health information.

Section 164.502(b)—Minimum Necessary

Comments on the minimum necessary standard are addressed in the preamble to § 164.514(d).

Section 164.502(c)—Uses or Disclosures of Protected Health Information Subject to an Agreed Upon Restriction

Comments on the agreed upon restriction standard are addressed in the preamble to § 164.522(a).

Section 164.502(d)—Uses and Disclosures of De-Identified Protected Health Information

Comments on the requirements for de-identifying information are addressed in the preamble to § 164.514(a)–(c).

Section 164.502(e)—Business Associates

Comments on business associates are addressed in the preamble to § 164.504(e).

Section 164.502(f)—Deceased Individuals

Comment: Most commenters on this topic generally did not approve of the Secretary's proposal with regard to protected health information about deceased individuals. The majority of these commenters argued that our proposal was not sufficiently protective of such information. Commenters agreed with the statements made in the preamble to the proposed rule that the privacy concerns addressed by this policy are not limited to the confidential protection of the deceased individual but instead also affects the decedent's family, as genetic information and information pertinent to hereditary diseases and risk factors for surviving relatives and direct family members may be disclosed through the disclosure of the deceased individual's confidential data. It was argued that the proposal would be inadequate to protect the survivors who could be negatively affected and in most cases will outlive the two-year period of protection. A number of medical associations asserted that individuals may avoid genetic testing, diagnoses, and treatment and suppress information important to their health care if they fear family members will suffer discrimination from the release of their medical information after their death. One commenter pointed out that ethically little distinction can be made between protecting an individual's health information during life and protecting it post-mortem. Further, it was argued that the privacy of the deceased individual and his or her family is far more important than allowing genetic information to be abstracted by an institutional or commercial collector of information. A few commenters asked that we provide indefinite protection on the protected health information about a deceased person contained in psychotherapy notes. One commenter asked that we extend protections on records of children who have died of cancer for the lifetime of a deceased child's siblings and parents.

The majority of commenters who supported increased protections on the protected health information about the deceased asked that we extend protections on such information indefinitely or for as long as the covered entity maintains the information. It was also argued that the administrative burden of perpetual protection would be no more burdensome than it is now as current practice is that the confidentiality of identifiable patient information continues after death. A number of others pointed out that there was no reason to set a different privacy standard for deceased individuals than we had for living individuals and that it has been standard practice to release the information of deceased individuals with a valid consent of the executor, next of kin, or specific court order. In addition, commenters referenced Hawaii's health care information privacy law (see Haw. Rev. Stat. section

323C–43) as at least one example of a state law where the privacy and access provisions of the law continue to apply to the protected health information of a deceased individual following the death of that individual.

Response: We find the arguments raised by these commenters persuasive. We have reconsidered our position and believe these arguments for maintaining privacy on protected health information without temporal limitations outweigh any administrative burdens associated with maintaining such protections. As such, in the final rule we revise our policy to extend protections on the protected health information about a deceased individual to remain in effect for as long as the covered entity maintains the information.

For purposes of this regulation, this means that, except for uses and disclosures for research purposes (see § 164.512(i)), covered entities must under this rule protect the protected health information about a deceased individual in the same manner and to the same extent as required for the protected health information of living individuals. This policy alleviates the burden on the covered entity from having to determine whether or not the person has died and if so, how long ago, when determining whether or not the information can be released.

Comment: One commenter asked us to delete our standard for deceased individuals, asserting that the deceased have no constitutional right to privacy and state laws are sufficient to maintain protections for protected health information about deceased individuals.

Response: We understand that traditional privacy law has historically stripped privacy protection on information at the time the subject of the information dies. However, as we pointed out in the preamble to the proposed rule, the dramatic proliferation of electronic-based interchanges and maintenance of information has enabled easier and more ready access to information that once may have been de facto protected for most people because of the difficulty of its collection and aggregation. It is also our understanding that current state laws vary widely with regard to the privacy protection of a deceased individual's individually identifiable health information. Some are less protective than others and may not take into account the implications of disclosure of genetic and hereditary information on living individuals. For these reasons, a regulatory standard is needed here in order to adequately protect the privacy interests of those who are living.

Comment: Another commenter expressed concern over the administrative problems that the proposed standard would impose, particularly in the field of retrospective health research.

Response: For certain research purposes, we permit a covered entity to use and disclose the protected health information of a deceased individual without authorization by a personal representative and absent review by an IRB or privacy board. The verification standard (§ 164.514(h)) requires that covered entities obtain an oral or written representation that the protected health information sought will be used or disclosed solely for research, and § 164.512(i)(1)(iii) requires the covered entity to obtain from the researcher documentation of the death of the individual. We believe the burden on the covered entity will be small, because it can reasonably rely on the representation of purpose and documentation of death presented by the researcher.

Comment: A few commenters argued that the standard in the proposed rule would cause significant administrative burdens on their record retention and storage policies. Commenters explained that they have internal policy record-retention guidelines which do not envision the retention of records beyond a few years. Some commenters complained about the burden of having to track dates of death, as the commenters are not routinely notified when an individual has died.

Response: The final rule does not dictate any record retention requirements for the records of deceased individuals. Since we have modified the NPRM to cover protected health information about deceased individuals for as long as the covered entity maintains the information, there will be no need for the covered entity to track dates of death.

Comment: A few commenters voiced support for the approach proposed in the proposal to maintain protections for a period of two years.

Response: After consideration of public comments, we chose not to retain this approach because the two-year period would be both inadequate and arbitrary. As discussed above, we agree with commenter arguments in support of providing indefinite protection.

Comment: A few commenters expressed concern that the regulations may be interpreted as providing a right of access to a deceased's records only for a two-year period after death. They asked the Department to clarify that the right of access of an individual, including the representatives of a deceased individual, exists for the entire period the information is held by a covered entity.

Response: We agree with these comments, given the change in policy discussed above.

Comment: A few commenters suggested that privacy protections on protected health information about deceased individuals remain in effect for a specified time period longer than 2 years, arguing that two years was not long enough to protect the privacy rights of living individuals. These commenters, however, were not in agreement as to what other period of protection should be imposed, suggesting various durations from 5 to 20 years.

Response: We chose not to extend protections in this way because specifying another time period would raise many of the same concerns voiced by the commenters regarding our proposed two year period and would not reduce the administrative burden of having to track or learn dates of death. We believe that the policy in this final rule extending protections for as long as the covered entity maintains the information addresses commenter concerns regarding the need for increased protections on the protected health information about the deceased.

Comment: Some commenters asserted that information on the decedent from the death certificate is important for assessment and research purposes and requested that the Department clarify accordingly that death certificate data be allowed for use in traditional public health assessment activities.

Response: Nothing in the final rule impedes reporting of death by covered entities as required or authorized by other laws, or access to death certificate data to the extent that such data is available publicly from non-covered entities. Death certificate data maintained by a covered entity is protected health information and must only be used or disclosed by a covered entity in accordance with the requirements of this regulation. However, the final rule permits a covered entity to disclose protected health information about a deceased individual for research purposes without authorization and absent IRB or privacy board approval.

Comment: A few commenters asked that we include in the regulation a mechanism to provide for notification of date of death. These commenters questioned how a covered entity or business partner would be notified of a death and subsequently be able to determine whether the two-year period of protection had expired and if they

were permitted to use or disclose the protected health information about the deceased. One commenter further stated that absent such a mechanism, a covered entity would continue to protect the information as if the individual were still living. This commenter recommended that the burden for providing notification and confirmation of death be placed on any authorized entity requesting information from the covered entity beyond the two-year period.

Response: In general, such notification is no longer necessary as, except for uses and disclosures for research purposes, the final rule protects the protected health information about a deceased individual for as long as the covered entity holds the record. With regard to uses and disclosures for research, the researcher must provide covered entities with appropriate documentation of proof of death, the burden is not on the covered entity.

Comment: A few commenters pointed to the sensitivity of genetic and hereditary information and its potential impact on the privacy of living relatives as a reason for extending protections on the information about deceased individuals for as long as the covered entity maintains the information. However, a few commenters recommended additional protections for genetic and hereditary information. For example, one commenter suggested that researchers should be able to use sensitive information of the deceased but then be required to publish findings in de-identified form. Another commenter recommended that protected health information about a deceased individual be protected as long as it implicates health problems that could be developed by living relatives.

Response: We agree with many of the commenters regarding the sensitivity of genetic or hereditary information and, in part for this reason, extended protections on the protected health information of deceased individuals. Our reasons for retaining the exception for research are explained above.

We agree with and support the practice of publishing research findings in de-identified form. However, we cannot regulate researchers who are not otherwise covered entities in this regulation.

Comment: One commenter asked that the final rule allow for disclosure of protected health information to funeral directors as necessary for facilitating funeral and disposition arrangements. The commenter believed that our proposal could seriously disrupt a family's ability to make funeral arrangements as hospitals, hospices, and other health care providers would not be allowed to disclose the time of death and other similar information critical to funeral directors for funeral preparation. The commenter also noted that funeral directors are already precluded by state licensing regulations and ethical standards from inappropriately disclosing confidential information about the deceased.

Further, the commenter stated that funeral directors have legitimate needs for protected health information of the deceased or of an individual when death is anticipated. For example, often funeral directors are contacted when death is foreseen in order to begin the process of planning funeral arrangements and prevent unnecessary delays. In addition, the embalming of the body is affected by the medical condition of the body.

In addition, it was noted that funeral directors need to be aware of the presence of a contagious or infectious disease in order to properly advise family members of funeral and disposition options and how they may be affected by state law. For example, certain states may prohibit cremation of remains for a certain period unless the death was caused by a contagious or infectious disease, or prohibit family members from assisting in preparing the body for disposition if there is a risk of transmitting a communicable disease from the corpse.

Response: We agree that disclosures to funeral directors for the above purposes should be allowed. Accordingly, the final rule at § 164.512(g)(2) permits covered entities to disclose protected health information to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. Such disclosures are also permitted prior to, and in reasonable anticipation of, the individual's death.

Comment: Several commenters urged that the proposed standard for deceased individuals be clarified to allow access by a family member who has demonstrated a legitimate health-related reason for seeking the information when there is no executor, administrator, or other person authorized under applicable law to exercise the right of access of the individual.

Another commenter asked that the rule differentiate between blood relatives and family members and address their different access concerns, such as with genetic information versus information about transmittable diseases. They also recommended that the regulation allow access to protected health information by blood-related relatives prior to the end of the two-year period and provide them with the authority to extend the proposed two-year period of protection if they see fit. Lastly, the commenter suggested that the regulation address the concept of when the next-of-kin may not be appropriate to control a deceased person's health information.

Response: We agree that family members may need access to the protected health information of a deceased individual, and this regulation permits such disclosure in two ways. First, a family member may qualify as a ''personal representative'' of the individual (see § 164.502(g)). Personal representatives include anyone who has authority to act on behalf of a deceased individual or such individual's estate, not just legally-appointed executors. We also allow disclosure of protected health information to health care providers for purposes of treatment, including treatment of persons other than the individual. Thus, where protected health information about a deceased person is relevant to the treatment of a family member, the family member's physician may obtain that information. Because we limit these disclosures to disclosures for treatment purposes, there is no need to distinguish between disclosure of information about communicable diseases and disclosure of genetic information.

With regard to fitness to control information, we defer to existing state and other laws that address this matter.

Section 164.502(g)—Personal Representative

Comment: It was observed that under the proposed regulation, legal representatives with ''power of attorney'' for matters unrelated to health care would have unauthorized access to confidential medical records. Commenters recommended that access to a person's protected health information be limited to those representatives with a ''power of attorney'' for health care matters only. Related comments asked that the rule limit the definition of ''power of attorney'' to include only those instruments granting specific power to deal with health care functions and health care records.

Response: We have deleted the reference to ''power of attorney.'' Under the final rule, a person is a personal representative of a living individual if, under applicable law, such person has authority to act on behalf of an individual in making decisions related to health care. ''Decisions relating to health care'' is broader than consenting to treatment on behalf of an individual;

for example, it would include decisions relating to payment for health care. We clarify that the rights and authorities of a personal representative under this rule are limited to protected health information relevant to the rights of the person to make decisions about an individual under other law. For example, if a husband has the authority only to make health care decisions about his wife in an emergency, he would have the right to access protected health information related to that emergency, but he may not have the right to access information about treatment that she had received ten years ago.

We note that the rule for deceased individuals differs from that of living individuals. A person may be a personal representative of a deceased individual if they have the authority to act on behalf of such individual or such individual's estate for any decision, not only decisions related to health care. We create a broader scope for a person who is a personal representative of a deceased individual because the deceased individual can not request that information be disclosed pursuant to an authorization, whereas a living individual can do so.

Comment: Some commenters asked that the NPRM provision allowing informal decision-makers access to the protected health information of an incapacitated individual should be maintained in the final rule.

Response: We agree with the commenters, and retain permission for covered entities to share protected health information with informal decision-makers, under conditions specified in § 164.510(b). A person need not be a personal representative for such disclosure of protected health information to be made to an informal decision-maker.

Comment: Commenters urged that individuals with mental retardation, who can provide verbal agreement or authorization, should have control over dissemination of their protected health information, in order to increase the privacy rights of such individuals.

Response: Individuals with mental retardation have control over dissemination of their protected health information under this rule to the extent that state law provides such individuals with the capacity to act on their own behalf. We note that a covered entity need not disclose information pursuant to a consent or authorization. Therefore, even if state law determines that an individual with mental retardation is not competent to act and a personal representative provides authorization for a disclosure, a covered entity may choose not to disclose such information if the individual who lacks capacity to act expresses his or her desire that such information not be disclosed.

Comment: A commenter suggested that the final rule should provide health plans with a set of criteria for formally identifying an incapacitated individual's decision-maker. Such criteria would give guidance to health plans that would help in not releasing information to the wrong person.

Response: The determination about who is a personal representative under this rule is based on state or other applicable law. We require that a covered entity verify the authority of a personal representative, in accordance with § 164.514(h) in order to disclose information to such person.

Comment: Commenters were troubled by the inclusion of minors in the definition of ''individual'' and believed that the presumption should be that parents have the right to care for their children.

Response: We agree that a parent should have access to the protected health information about their unemancipated minor children, except in limited circumstances based on state law. The approach in the final rule helps clarify this policy. The definition of ''individual'' is simplified in the final rule to ''the person who is the subject of protected health information.'' (§ 164.501). We created a new section (§ 164.502(g)) to address ''personal representatives,'' which includes parents and guardians of unemancipated minors. Generally, we provide that if under applicable law a parent has authority to act on behalf of an unemancipated minor in making decisions relating to health care about the minor, a covered entity must treat the parent as the personal representative with respect to protected health information relevant to such personal representation. The regulation provides only three limited exceptions to this rule based upon current state law and physician practice.

Comment: Many commenters agreed with our approach in the NPRM to give minors who may lawfully access health care the rights to control the protected health information related to such health care.

Several commenters disagreed with this approach and recommended that where states allow minors too much independence from parents, the rule should not defer to state law. One commenter suggested that we give an individual the right to control protected health information only when the individual reaches the age of majority.

Response: In the final rule, the parent, as the personal representative of a minor child, controls the protected health information about the minor, except that the parent does not act as a personal representative of the minor under the rule in three limited circumstances based on state consent law and physician practice. The final rule defers to consent laws of each state and does not attempt to evaluate the amount of control a state gives to a parent or minor. If a state provides an alternative means for a minor to obtain health care, other than with the consent of a parent, this rule preserves the system put in place by the state.

The first two exceptions, whereby a parent is not the personal representative for the minor and the minor can act for himself or herself under the rule, occur if the minor consents to a health care service, and no other consent to such health care service is required by law, or when the minor may lawfully obtain a health care service without the consent of a parent, and the minor, a court, or another person authorized by law consents to such service. The third exception is based on guidelines of the American Pediatric Association, current practice, and agreement by parents. If a parent assents to an agreement of confidentiality between a covered provider and a minor with respect to a health care service, the parent is not the personal representative of the minor with respect to the protected health information created or received subject to that confidentiality agreement. In such circumstances, the minor would have the authority to act as an individual, with respect to such protected health information.

Comment: Some commenters requested that we permit minors to exercise the rights of an individual when applicable law requires parental notification as opposed to parental consent.

Response: We adopt this policy in the final rule. If the minor consents to a health care service, and no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained or notification to another person has been given, only the minor may be treated as the individual with respect to the protected health information relating to such health care service. The rule does not affect state law that authorizes or requires notification to a parent of a minor's decision to obtain a health care service to the extent authorized or required by such law. In addition, state parental notification laws do not affect the rights of minors under this regulation.

Comment: Some commenters requested clarification that when a minor may obtain a health care service without parental consent and voluntarily chooses to involve a parent, the minor retains the rights, authorities and confidentiality protections established in this rule.

Response: We agree that minors should be encouraged to voluntarily involve a parent or other responsible adult in their health care decisions. The rule is not intended to require that minors choose between involving a parent and maintaining confidentiality protections. We have added language in § 164.502(g)(3)(i) to clarify that when a minor consents to a health care service and no other consent is required by law, if the minor voluntarily chooses to involve a parent or other adult, the minor nonetheless maintains the exclusive ability to exercise their rights under the rule. This is true even if a parent or other person also has consented to the health care service for which the minor lawfully consented. Under the rule, a minor may involve a parent and still preserve the confidentiality of their protected health information. In addition, a minor may choose to have a parent act as his or her personal representative even if the minor could act on his or her own behalf under the rule. If the minor requests that a covered entity treat a parent as his or her personal representative, the covered entity must treat such person as the minor's personal representative even if the minor consents to a health care service and no other consent to such health care service is required by law.

Comment: Some commenters requested that the rule provide for the preservation of patient confidences if a health care provider and a minor patient enter into an agreement of confidentiality and a parent assents to this arrangement.

Response: We have addressed this concern in the final rule by adding a provision that ensures that a minor maintains the confidentiality protections provided by the rule for information that is created or received pursuant to a confidential communication between a provider and a minor when the minor's parent assents to an agreement of confidentiality between the provider and the minor. (§ 164.502(g)(3)(ii)). The American Academy of Pediatrics Guidelines for Health Supervision III, which are meant to serve as ''a framework to help clinicians focus on important issues at developmentally appropriate time intervals,'' recommends that physicians interview children alone beginning at the age of twelve (or as early as the age of ten if it is comfortable for the child). This recommendation is based on the fact that adolescents tend to underutilize existing health care resources, in part, because of a concern for confidentiality.[7] The recommended interview technique in the Guidelines states that the provider discuss the rules of confidentiality with the adolescent and the parent and that the adolescent's confidentiality should be respected. We do not intend to interfere with these established protocols or current practices. Covered entities will need to establish procedures to separate protected health information over which the minor maintains control from protected health information with respect to which the minor's parent has rights as a personal representative of the minor.

A covered provider may disclose protected health information to a parent, regardless of a confidentiality agreement, if there is an imminent threat to the minor or another person, in accordance with § 164.512(j)(1)(i).

Comment: Several commenters suggested that we add a provision in the final rule to provide minors and parents with concurrent rights under certain circumstances, particularly when the minor reaches 16 years of age or when a parent authorizes his or her minor child to exercise these rights concurrently.

Response: We do not add such provision in the final rule. We believe that establishing concurrent rights through this rule could result in problems that effect the quality of health care if the minor and the parent were to disagree on the exercise of their rights. The rule would not prevent a parent from allowing a minor child to make decisions about his or her protected health information and acting consistently with the minor's decision. In all cases, either the parent has the right to act for the individual with respect to protected health information, or the minor has the right to act for himself or herself. The rule does not establish concurrent rights for parents and minors.

Comment: Commenters requested clarification about the rights of an adult or emancipated minor with respect to protected health information concerning health care services rendered while the person was an unemancipated minor.

Response: Once a minor becomes emancipated or attains the age of majority, as determined by applicable state law, the parent is no longer the personal representative under § 164.502(g)(3) of such individual, unless the parent has the authority to act on behalf of the individual for some reason other than their authority as a parent. An adult or emancipated minor has rights under the rule with respect to all protected health information about them, including information obtained while the individual was an unemancipated minor.

Comment: One commenter pointed out that language in the definition of individual in the NPRM that grants a minor the rights of an individual when he or she ''lawfully receives care without the consent of, or notification to, a parent * * *'' would have the effect of granting rights to an infant minor who receives emergency care when the parent is not available.

Response: This result was not our intent. We have changed the language in § 164.502(g)(3)(i) of the final rule to provide a minor the right to act as an individual when the minor can obtain care without the consent of a parent and the minor consents to such care. Because an infant treated in an emergency situation would not be able to consent to care, the infant's parent would be treated as the personal representative of the infant. Section 164.502(g)(3)(ii) provides that the parent is not the personal representative of the minor under the rule if the minor may obtain health care without the consent of a parent and the minor, a court, or another person authorized by law consents to such service. If an infant obtains emergency care without the consent of a parent, a health care provider may provide such care without consent to treatment. This situation would fall outside the second exception, and the parent would remain the personal representative of the minor.

Comment: Commenters were concerned about the interaction of this rule with FERPA with respect to parents' right to access the medical records of their children.

Response: We direct the commenters to a discussion of the interaction between our rule and FERPA in the ''Relationship to Other Federal Laws'' section of the preamble.

Section 164.502(h)—Confidential Communications

Comments on confidential communications are addressed in the preamble to § 164.522(b).

[7] Confidentiality in Adolescent Health Care, a joint policy statement of the American Academy of Pediatrics; the American Academy of Family Physicians; the American College of Obstetricians and Gynecologists; NAACOG—The Organization for Obstetric, Gynecologic, and Neonatal Nurses; and the National Medical Association.

Section 164.502(i)—Uses and Disclosures Consistent With Notice

Comments on the notice requirements are addressed in the preamble to § 164.520.

Section 164.502(j)—Uses and Disclosures by Whistleblowers and Workforce Crime Victims

Comments: Some commenters wanted to see more limitations put on the ability to whistleblow in the final rule. These commenters were concerned about how disclosed protected health information would be used during and subsequent to the whistleblowing event and felt that adding additional limitations to the ability to whistleblow would help to alleviate these concerns. Some of these commenters were concerned that there was no protection against information later being leaked to the public or re-released after the initial whistleblowing event, and that this could put covered entities in violation of the law. Many commenters wanted to see the whistleblower provision deleted entirely. According to a number of health care associations who commented on this topic, current practices already include adequate mechanisms for informing law enforcement, oversight and legal counsel of possible violations without the need for patient identifiable information; thus, the provision allowing whistleblowers to share protected health information is unnecessary. Additionally, some commenters felt that the covered entity needs to be allowed to prohibit disclosures outside of legitimate processes. Some commenters were concerned about not having any recourse if the whistleblower's suspicions were unfounded.

Response: In this rule, we do not regulate the activities of whistleblowers. Rather, we regulate the activities of covered entities, and determine when they may be held responsible under this rule for whistleblowing activities of their workforce or business associates when that whistleblowing involves the disclosure of protected health information. Similarly, we regulate when covered entities must and need not sanction their workforce who disclose protected health information in violation of the covered entity's policies and procedures, when that disclosure is for whistleblowing purposes. See § 164.530(e). This rule does not address a covered entity's recourse against a whistleblower under other applicable law.

We do not hold covered entities responsible under this rule for whistleblowing disclosures of protected health information under the circumstances described in § 164.502(j). Our purpose in including this provision is to make clear that we are not erecting a new barrier to whistleblowing, and that covered entities may not use this rule as a mechanism for sanctioning workforce members or business associates for whistleblowing activity. We do not find convincing commenters' arguments for narrowing or eliminating the scope of the whistleblowing which triggers this protection.

Congress, as well as several states, have recognized the importance of whistleblower activity to help identify fraud and mismanagement and protect the public's health and safety. Whistleblowers, by their unique insider position, have access to critical information not otherwise easily attainable by oversight and enforcement organizations.

While we recognize that in many instances, de-identified or anonymous information can be used to accomplish whistleblower objectives, there are instances, especially involving patient care and billing, where this may not be feasible. Oversight investigative agencies such as the Department of Justice rely on identifiable information in order to issue subpoenas that are enforceable. Relevant court standards require the government agency issuing the subpoena to explain why the specific records requested are relevant to the subject of the investigation, and without such an explanation the subpoena will be quashed. Issuing a subpoena for large quantities of individual records to find a few records involving fraud is cost prohibitive as well as likely being unenforceable.

We note that any subsequent inappropriate disclosure by a recipient of whistleblower information would not put the covered entity in violation of this rule, since the subsequent disclosure is not covered by this regulation.

Comments: A few commenters felt that the whistleblower should be held to a ''reasonableness standard'' rather than a ''belief'' that a violation has taken place before engaging in whistleblower activities. The commenters felt that a belief standard is too subjective. By holding the whistleblower to this higher standard, this would serve to protect protected health information from being arbitrarily released. Some commenters saw the whistleblower provision as a loophole that gives too much power to disgruntled employees to inappropriately release information in order to cause problems for the employer.

On the other hand, some commenters felt that all suspicious activities should be reported. This would ease potential whistleblowers' concerns over whether or not they had a legitimate concern by leaving this decision up to someone else. A number of commenters felt that employees should be encouraged to report violations of professional or clinical standards, or when a patient, employee, or the public would be put at risk. A small number of commenters felt that the whistleblower should raise the issue within the covered entity before going to the attorney, oversight agency, or law enforcement entity.

Response: We do not attempt to regulate the conduct of whistleblowers in this rule. We address uses and disclosures of protected health information by covered entities, and when a covered entity will violate this rule due to the actions of a workforce member or business associate. In the final rule, we provide that a covered entity is not in violation of the rule when a workforce member or business associate has a good faith belief that the conduct being reported is unlawful or otherwise violates professional or clinical standards, or potentially endangers patients, employees or the public. We concur that the NPRM language requiring only a ''belief'' was insufficient. Consequently, we have strengthened the standard to require a good faith belief that an inappropriate behavior has occurred.

Comment: A number of commenters believe that employees should be encouraged to report violations of professional or clinical standards, or report situations where patients, employees, or the public would be put at risk. Their contention is that employees, especially health care employees, may not know whether the problem they have encountered meets a legal threshold of wrongdoing, putting them at jeopardy of sanction if they are incorrect, even if the behavior did reflect violation of professional and clinical standards or put patients, employees, or the public at risk.

Response: We agree that covered entities should be protected when their employees and others engage in the conduct described by these commenters. We therefore modify the proposal to protect covered entities when the whistleblowing relates to violations of professional or clinical standards, or situations where the public may be at risk, and eliminate the reference to ''evidence.''

Comments: A significant number of those commenting on the whistleblower provision felt that this provision was contrary to the rest of the rule.

Whistleblowers could very easily release protected health information under this provision despite the fact that the rest of this rule works very hard to ensure privacy of protected health information in all other contexts. To this end, some commenters felt that whistleblowers should not be exempt from the minimum necessary requirement.

Response: As stated above, we do not regulate the conduct of whistleblowers. We discuss above the importance of whistleblowing, and our intention not to erect a new barrier to such activity. The minimum necessary standard applies to covered entities, not to whistleblowers.

Comments: Some commenters felt that disclosures of suspected violations should only be made to a law enforcement official or oversight agency. Other commenters said that whistleblowers should be able to disclose their concerns to long-term care ombudsmen or health care accreditation organizations, particularly because certain protected health information may contain evidence of abuse. Some commenters felt that whistleblowers should not be allowed to freely disclose information to attorneys. They felt that this may cause more lawsuits within the health care industry and be costly to providers. Furthermore, allowing whistleblowers to go to attorneys increases the number of people who have protected health information without any jurisdiction for the Secretary to do anything to protect this information.

Response: We agree with the commenters who suggested that we recognize other appropriate entities to which workforce members and business associates might reasonably make a whistleblowing disclosure. In the final rule we expand the provision to protect covered entities for disclosures of protected health information made to accreditation organizations by whistleblowers. We agree with the commenters that whistleblowers may see these organizations as appropriate recipients of health information, and do not believe that covered entities should be penalized for such conduct.

We also agree that covered entities should be protected when whistleblowers disclose protected health information to any health oversight agency authorized by law to investigate or oversee the conditions of the covered entity, including state Long-Term Care Ombudsmen appointed in accordance with the Older Americans Act. Among their mandated responsibilities is their duty to identify, investigate and resolve complaints that are made by, or on behalf of, residents related to their health, safety, welfare, or rights. Nursing home staff often bring complaints regarding substandard care or abuse to ombudsmen. Ombudsmen provide a potentially more attractive outlet for whistleblowers since resolution of problems may be handled short of legal action or formal investigation by an oversight agency.

We disagree with commenters that the provision permitting disclosures to attorneys is too broad. Workforce members or business associates may not understand their legal options or their legal exposure when they come into possession of information about unlawful or other inappropriate or dangerous conduct. Permitting potential whistleblowers to consult an attorney provides them with a better understanding of their legal options. We rephrase the provision to improve its clarity.

Comment: One commenter suggested that a notice of information practices that omits disclosure for voluntary reporting of fraud will chill internal whistleblowers who will be led to believe—falsely—that they would violate federal privacy law, and be lawfully subject to sanction by their employer, if they reported fraud to health oversight agencies.

Response: The notice of information practices describes a covered entity's information practices. A covered entity does not make whistleblower disclosures of protected health information, nor can it be expected to anticipate any such disclosures by its workforce.

Comment: One commenter suggested that the whistleblower provisions could allow covered entities to make illegal disclosures to police through the back door by having an employee who believes there is a violation of law do the disclosing. Any law could have been violated and the violator could be anyone (a patient, a member of the patient's family, etc.)

Response: We have eliminated whistleblower disclosures for law enforcement purposes from the list of circumstances in which the covered entity will be protected under this rule. This provision is intended to protect the covered entity when a member of its workforce or a business associate discloses protected health information to whistleblow on the covered entity (or its business associates); it is not intended for disclosures of conduct by the individual who is the subject of the information or third parties.

Section 164.504—Uses and Disclosures—Organizational Requirements—Component Entities, Affiliated Entities, Business Associates and Group Health Plans

Section 164.504(a)–(c)—Health Care Component (Component Entities) and Section 164.504(d)—Affiliated Entities

Comment: A few commenters asked that the concept of ''use'' be modified to allow uses within an integrated healthcare delivery system. Commenters argued that the rule needs to ensure that the full spectrum of treatment is protected from the need for authorizations at the points where treatment overlaps entities. It was explained that, for example, treatment for a patient often includes services provided by various entities, such as by a clinic and hospital, or that treatment may also necessitate referrals from one provider entity to another unrelated entity. Further, the commenter argued that the rule needs to ensure that the necessary payment and health care operations can be carried out across entities without authorizations.

Response: The Department understands that in today's health care industry, the organization of and relationships among health care entities are highly complex and varied. We modify the proposed rule significantly to allow affiliated entities to designate themselves as a single covered entity. A complex organization, depending on how it self-designates, may have one or several ''health care component(s)'' that are each a covered entity. Aggregation into a single covered entity will allow the entities to use a single notice of information practices and will allow providers that must obtain consent for uses and disclosures for treatment, payment, and operations to obtain a single consent.

We do not allow this type of aggregation for unrelated entities, as suggested by some commenters, because unrelated entities' information practices will be too disparate to be accurately reflected on a single consent or notice form. Our policies on when consent and authorization are required for sharing information among unrelated entities, and the rationale for these policies, is described in §§ 164.506 and 164.508 and corresponding preamble.

As discussed above, in the final rule we have added a definition of organized health care arrangement and permit covered entities participating in such arrangements to disclose protected health information to support the health care operations of the arrangement. See the preamble discussion of the definitions of organized health care

arrangement and health care operations, § 164.501.

Comment: Some commenters expressed concern that the requirement to obtain authorization for the disclosure of information to a non-health related division of the covered entity would impede covered entities' ability to engage in otherwise-permissible activities such as health care operations. Some of these commenters requested clarification that covered entities are only required to obtain authorization for disclosures to non-health related divisions if the disclosure is for marketing purposes.

Response: In the final rule, we remove the example of use and disclosure to non-health related divisions of the covered entity from the list of examples of uses and disclosures requiring authorization in § 164.508. We determined that the example could lead covered entities to the mistaken conclusion that some uses or disclosures that would otherwise be permitted under the rule without authorization would require authorization when made to a non-health related division of the covered entity. In the final rule, we clarify that disclosure to a non-health related division does not require authorization if the use or disclosure is otherwise permitted or required under the rule. For example, in § 164.501 we define health care operations to include conducting or arranging for legal and auditing services. A covered entity that is the health care component of a larger entity is permitted under the final rule to include the legal department of the larger entity as part of the health care component. The covered entity may not, however, generally permit the disclosure of protected health information from the health care component to non-health related divisions unless they support the functions of the health care component and there are policies and procedures in place to restrict the further use to the support of the health related functions.

Comment: Many commenters, especially those who employed providers, supported our position in the proposed rule to consider only the health care component of an entity to be the covered entity. They stated that this was a balanced approach that would allow them to continue conducting business. Some commenters felt that there was ambiguity in the regulation text of the proposed rule and requested that the final rule explicitly clarify that only the health care component is considered the covered entity, not the entity itself. Similarly, another commenter requested that we clarify that having a health care component alone did not make the larger entity a covered entity under the rule.

Response: We appreciate the support of the commenters on the health care component approach and we agree that there was some ambiguity in the proposed rule. The final rule creates a new § 164.504(b) for health care components. Under § 164.504(b), for a covered entity that is a single legal entity which predominantly performs functions other than the functions performed by a health plan, provider, or clearinghouse, the privacy rules apply only to the entity's health care component. A policy, plan, or program that is an ''excepted benefit'' under section 2791(c)(1) of HIPAA cannot be part of a health care component because it is expressly excluded from the definition of ''health plan'' for the reasons discussed above. The health care component is prohibited from sharing protected health information outside of the component, except as otherwise permitted or required by the regulation.

At a minimum, the health care component includes the organizational units of the covered entity that operate as or perform the functions of the health plan, health care provider, or clearinghouse and does not include any unit or function of the excepted benefits plan, policy, or program. While the covered entity remains responsible for compliance with this rule because it is responsible for the actions of its workforce, we otherwise limit the responsibility to comply to the health care component of the covered entity. The requirements of this rule apply only to the uses and disclosures of the protected health information by the component entity. See § 164.504(b).

Comment: Some commenters stated that the requirement to erect firewalls between different components would unnecessarily delay treatment, payment, and health care operations and thereby increase costs. Other commenters stressed that it is necessary to create firewalls between the health care component and the larger entity to prevent unauthorized disclosures of protected health information.

Response: We believe that the requirement to implement firewalls or safeguards is necessary to provide meaningful privacy protections, particularly because the health care component is part of a larger legal organization that performs functions other than those covered under this rule. Without the safeguard requirement we cannot ensure that the component will not share protected health information with the larger entity. While we do not specifically identify the safeguards that are required, the covered entity must implement policies and procedures to ensure that: the health care component's use and disclose of protected health information complies with the regulation; members of the health care component who perform duties for the larger entity do not use and disclose protected health information obtained through the health care component while performing non-component functions unless otherwise permitted or required by the regulation; and when a covered entity conducts multiple functions regulated under this rule, the health care component adheres to the appropriate requirements (e.g. when acting as a health plan, adheres to the health plan requirements) and uses or discloses protected health information of individuals who receive limited functions from the component only for the appropriate functions. See §§ 164.504(c)(2) and 164.504(g). For example, a covered entity that includes both a hospital and a health plan may not use protected health information obtained from an individual's hospitalization for the health plan, unless the individual is also enrolled in the health plan. We note that covered entities are permitted to make a disclosure to a health care provider for treatment of an individual without restrictions.

Comment: One commenter stated that multiple health care components of a single organization should be able to be treated as a single component entity for the purposes of this rule. Under this approach, they argued, one set of policies and procedures would govern the entire component and protected health information could be shared among components without authorization. Similarly, other commenters stated that corporate subsidiaries and affiliated entities should not be treated as separate covered entities.

Response: We agree that some efficiencies may result from designating multiple component entities as a single covered entity. In the final rule we allow legally distinct covered entities that share common ownership or control to designate themselves or their health care components as a single covered entity. See § 164.504(d). Common ownership is defined as an ownership or equity interest of five percent or more. Common control exists if an entity has the power—directly or indirectly—to significantly influence or direct the actions or policies of another entity. If the affiliated entity contains health care components, it must implement safeguards to prevent the

larger entity from using protected health information maintained by the component entity. As stated above, organizations that perform multiple functions may designate a single component entity as long as it does not include the functions of an excepted benefit plan that is not covered under the rule. In addition, it must adhere to the appropriate requirements when performing its functions (e.g. when acting as a health plan, adhere to the health plan requirements) and uses or discloses protected health information of individuals who receive limited functions from the component only for the appropriate functions. At the same time, a component that is outside of the health care component may perform activities that otherwise are not permitted by a covered entity, as long as it does not use or disclose protected health information created or received by or on behalf of the health care component in ways that violate this rule.

Comment: Some commenters asked whether or not workers' compensation carriers could be a part of the health care component as described in the proposed rule. They argued that this would allow for sharing of information between the group health plan and workers' compensation insurers.

Response: Under HIPAA, workers' compensation is an excepted benefit program and is excluded from the definition of ''health plan.'' As such, a component of a covered entity that provides such excepted benefits may not be part of a health care component that performs the functions of a health plan. If workforce members of the larger entity perform functions for both the health care component and the non-covered component, they may not use protected health information created or received by or on behalf of the health care component for the purposes of the non-covered component, unless otherwise permitted by the rule. For example, information may be shared between the components for coordination of benefits purposes.

C*omment:* Several commenters requested specific guidance on identifying the health care component entity. They argued that we underestimated the difficulty in determining the component and that many organizations have multiple functions with the same people performing duties for both the component and the larger entity.

Response: With the diversity of organizational structures, it is impossible to provide a single specific guidance for identifying health care components that will meet the needs of all organizations. Covered entities must designate their health care components consistent with the definition at § 164.504(a). We have tried to frame this definition to delineate what comes within a health care component and what falls outside the component.

Comment: A commenter representing a government agency recommended that only the component of the agency that runs the program be considered a covered entity, not the agency itself. In addition, this commenter stated that often subsets of other government agencies work in partnership with the agency that runs the program to provide certain services. For example, one state agency may provide maternity support services to the Medicaid program which is run by a separate agency. The commenter read the rule to mean that the agency providing the maternity support services would be a business associate of the Medicaid agency, but was unclear as to whether it would also constitute a health care component within its own agency.

Response: We generally agree. We expect that in most cases, government agencies that run health plans or provide health care services would typically meet the definition of a ''hybrid entity'' under § 164.504(a), so that such an agency would be required to designate the health care component or components that run the program or programs in question under § 164.504(c)(3), and the rules would not apply to the remainder of the agency's operations, under § 164.504(b). In addition, we have created an exception to the business associate contract requirement for government agencies who perform functions on behalf of other government agencies. Government agencies can enter into a memorandum of understanding with another government entity or adopt a regulation that applies to the other government entity in lieu of a business associate contract, as long as the memorandum or regulation contains certain terms. See § 164.504(e).

Comment: One commenter representing an insurance company stated that different product lines should be treated separately under the rule. For example, the commenter argued, because an insurance company offers both life insurance and health insurance, it does not mean that the insurance company itself is a covered entity, rather only the health insurance component is a covered entity. Another commenter requested clarification of the use of the term ''product line'' in the proposed rule. This commenter stated that product line should differentiate between different lines of coverage such as life vs. health insurance, not different variations of the same coverage, such as HMO vs. PPO. Finally, one commenter stated that any distinction among product lines is unworkable because insurance companies need to share information across product lines for coordinating benefits. This sharing of information, the commenter urged, should be able to take place whether or not all product lines are covered under the rule.

Response: We agree that many forms of insurance do not and should not come within the definition of ''health plan,'' and we have excepted them from the definition of this term in § 160.103 applies. This point is more fully discussed in connection with that definition. Although we do not agree that the covered entity is only the specific product line, as this comment suggests, the hybrid entity rules in § 164.504 address the substance of this concern. Under § 164.504(c)(3), an entity may create a health plan component which would include all its health insurance lines of business or separate health care components for each health plan product line. Finally, the sharing of protected health information across lines of business is allowed if it meets the permissive or required disclosures under the rule. The commenter's example of coordination of benefits would be allowed under the rule as payment.

Comment: Several commenters representing occupational health care providers supported our use of the component approach to prohibit unauthorized disclosures of protected health information. They requested that the regulation specifically authorize them to deny requests for disclosures outside of the component entity when the disclosure was not otherwise permitted or required by the regulation.

Response: We appreciate the commenters' support of the health care component approach. As members of a health care component, occupational health providers are prohibited from sharing protected health information with the larger entity (i.e., the employer), unless otherwise permitted or required by the regulation.

Comment: One commenter asked how the regulation affects employers who carry out research. The commenter questioned whether the employees carrying out the research would be component entities under the rule.

Response: If the employer is gathering its own information rather than obtaining it from an entity regulated by this rule, the information does not constitute protected health information since the employer is not a covered

entity. If the employer is obtaining protected health information from a covered entity, the disclosure by the covered entity must meet the requirements of § 164.512(i) regarding disclosures for research.

Comment: One commenter stated that the proposed rule did not clearly articulate whether employees who are health care providers are considered covered entities when they collect and use individually identifiable health information acting on behalf of an employer. Examples provided include, administering mandatory drug testing, making fitness-for-duty and return-to-work determinations, testing for exposure to environmental hazards, and making short and long term disability determinations. This commenter argued that if disclosing information gained through these activities requires authorization, many of the activities are meaningless. For example, an employee who fails a drug test is unlikely to give authorization to the provider to share the information with the employer.

Response: Health care providers are covered entities under this rule if they conduct standard transactions. A health care provider who is an employee and is administering drug testing on behalf of the employer, but does not conduct standard transactions, is not a covered entity. If the health care provider is a covered entity, then we require authorization for the provider to disclose protected health information to an employer. Nothing in this rule, however, prohibits the employer from conditioning an individual's employment on agreeing to the drug testing and requiring the individual to sign an authorization allowing his or her drug test results to be disclosed to the employer.

Comment: One commenter stated its belief that only a health center at an academic institution would be a covered entity under the component approach. This commenter believed it was less clear whether or not other components that may create protected health information ''incidentally'' through conducting research would also become covered entities.

Response: While a covered entity must designate as a health care component the functions that make it a health care provider, the covered entity remains responsible for the actions of its workforce. Components that create protected health information through research would be covered entities to the extent they performed one of the required transactions described in § 164.500; however, it is possible that the research program would not be part of the health care component, depending on whether the research program performed or supported covered functions.

Comment: Several commenters stated that employers need access to protected health information in order to provide employee assistance programs, wellness programs, and on-site medical testing to their employees.

Response: This rule does not affect disclosure of health information by employees to the employer if the information is not obtained from a covered entity. The employer's access to information from an EAP, wellness program, or on-site medical clinic will depend on whether the program or clinic is a covered entity.

Comment: One commenter stated that access to workplace medical records by the occupational medical physicians is fundamental to workplace and community health and safety. Access is necessary whether it is a single location or multiple sites of the same company, such as production facilities of a national company located throughout the country.

Response: Health information collected by the employer directly from providers who are not covered entities is outside the scope of this regulation. We note that the disclosures which this comment concerns should be covered by § 164.512(b).

Section 164.504(e)—Business Associates

Comment: Many commenters generally opposed the business partner standard and questioned the Secretary's legal authority under section 1172(a) of HIPAA to require business partner contracts. Others stated that the proposed rule imposed too great a burden on covered entities with regard to monitoring their business partners' actions. Commenters stated that they did not have the expertise to adequately supervise their business partners' activities—including billing, accounting, and legal activities—to ensure that protected health information is not inappropriately disclosed. Commenters argued that business partners are not ''under the control'' of health care providers, and that the rule would significantly increase the cost of medical care. Many commenters stated that the business partner provisions would be very time consuming and expensive to implement, noting that it is not unusual for a health plan or hospital to have hundreds of business partners, especially if independent physicians and local pharmacies are considered business partners. Many physician groups pointed out that their business partners are large providers, hospitals, national drug supplier and medical equipment companies, and asserted that it would be impossible, or very expensive, for a small physician group to attempt to monitor the activity of large national companies. Commenters stated that complex contract terms and new obligations would necessitate the investment of significant time and resources by medical and legal personnel, resulting in substantial expenses. Many commenters proposed that the duty to monitor be reduced to a duty to terminate the contractual arrangement upon discovery of a failure to comply with the privacy requirements.

In addition, many commenters argued that covered entities should have less responsibility for business partners' actions regarding the use and disclosure of protected health information. The proposed rule would have held covered entities responsible for the actions of their business partners when they ''knew or reasonably should have known'' of improper use of protected health information and failed to take reasonable steps to cure a breach of the business partner contract or terminate the contract. Many commenters urged that the term ''knew or should have known'' be clearly defined, with examples. Some commenters stated that covered entities should be liable only when they have actual knowledge of the material breach of the privacy rules by the business partner. Others recommended creation of a process by which a business partner could seek advice to determine if a particular disclosure would be appropriate. Some commenters stated that, in order to create an environment that would encourage covered entities to report misuses of protected health information, a covered entity should not be punished if it discovered an inappropriate disclosure.

Response: With regard to our authority to require business associate contracts, we clarify that Congress gave the Department explicit authority to regulate what uses and disclosures of protected health information by covered entities are ''authorized.'' If covered entities were able to circumvent the requirements of these rules by the simple expedient of contracting out the performance of various functions, these rules would afford no protection to individually identifiable health information and be rendered meaningless. It is thus reasonable to place restrictions on disclosures to business associates that are designed to ensure that the personal medical information disclosed to them continues to be protected and used and further

disclosed only for appropriate (i.e., permitted or required) purposes.

We do not agree that business associate contracts would necessarily have complex terms or result in significant time and resource burdens. The implementation specifications for business associate contracts set forth in § 164.504 are straightforward and clear. Nothing prohibits covered entities from having standard contract forms which could require little or no modification for many business associates.

In response to comments that the ''knew or should have known'' standard in the proposed rule was too vague or difficult to apply, and concerns that we were asking too much of small entities in monitoring the activities of much larger business associates, we have changed the rule. Under the final rule, we put responsibility on the covered entity to take action when it ''knew of a pattern of activity or practice of the business associate that constituted, respectively, a material breach or violation of the business associate's obligation under the contract * * *'' This will preclude confusion about what a covered entity 'should have known.' We interpret the term ''knew'' to include the situation where the covered entity has credible evidence of a violation. Covered entities cannot avoid responsibility by intentionally ignoring problems with their contractors. In addition, we have eliminated the requirement that a covered entity actively monitor and ensure protection by its business associates. However, a covered entity must investigate credible evidence of a violation by a business associate and act upon any such knowledge.

In response to the concern that the covered entity should not be punished if it discovers an inappropriate disclosure by its business associate, § 164.504(e) provides that the covered entity is not in compliance with the rule if it fails to take reasonable steps to cure the breach or end the violation, while § 164.530(f) requires the covered entity to mitigate, to the extent practicable, any resultant harm. The breach itself does not cause a violation of this rule.

Comment: Some commenters voiced support for the concept of business partners. Moreover, some commenters urged that the rule apply directly to those entities that act as business partners, by restricting disclosures of protected health information after a covered entity has disclosed it to a business partner.

Response: We are pleased that commenters supported the business associate standard and we agree that there are advantages to legislation that directly regulates most entities that use or disclose protected health information. However, we reiterate that our jurisdiction under the statute limits us to regulate only those covered entities listed in § 160.102.

Comment: Many commenters strongly opposed the provision in the proposed rule requiring business partner contracts to state that individuals whose protected health information is disclosed under the contract are intended third party beneficiaries of the contract. Many noted that HIPAA did not create a private right of action for individuals to enforce a right to privacy of medical information, and questioned the Secretary's authority to create such a right through regulation. Others questioned whether the creation of such a right was appropriate in light of the inability of Congress to reach consensus on the question, and perceived the provision as a ''back door'' attempt to create a right that Congress did not provide. Some commenters noted that third party beneficiary law varies from state to state, and that a third party beneficiary provision may be unenforceable in some states. These commenters suggested that the complexity and variation of state third party beneficiary law would increase cost and confusion with limited privacy benefits.

Commenters predicted that the provision would result in a dramatic increase in frivolous litigation, increased costs throughout the health care system, and a chilling effect on the willingness of entities to make authorized disclosures of protected information. Many commenters predicted that fear of lawsuits by individuals would impede the flow of communications necessary for the smooth operation of the health care system, ultimately affecting quality of care. For example, some predicted that the provision would inhibit providers from making authorized disclosures that would improve care and reduce medical errors. Others predicted that it would limit vendors' willingness to support information systems requirements. One large employer stated that the provision would create a substantial disincentive for employers to sponsor group health plans. Another commenter noted that the provision creates an anomaly in that individuals may have greater recourse against business partners and covered entities that contract with them than against covered entities acting alone.

However, some commenters strongly supported the concept of providing individuals with a mechanism to enforce the provisions of the rule, and considered the provision among the most important privacy protections in the proposed rule.

Response: We eliminate the requirement that business associate contracts contain a provision stating that individuals whose protected health information is disclosed under the contract are intended third-party beneficiaries of the contract.

We do not intend this change to affect existing laws regarding when individuals may be third party beneficiaries of contracts. If existing law allows individuals to claim third party beneficiary rights, or prohibits them from doing so, we do not intend to affect those rules. Rather, we intend to leave this matter to such other law.

Comment: Some commenters objected to the proposed rule's requirement that the business partner must return or destroy all protected health information received from the covered entity at the termination of the business partner contract. Commenters argued that business partners will need to maintain business records for legal and/or financial auditing purposes, which would preclude the return or destruction of the information. Moreover, they argued that computer back-up files may contain protected health information, but business partners cannot be expected to destroy entire electronic back-up files just because part of the information that they contain is from a client for whom they have completed work.

Response: We modify the proposed requirement that the business associate must return or destroy all protected health information received from the covered entity when the business associate contract is terminated. Under the final rule, a business associate must return or destroy all protected health information when the contract is terminated if feasible and lawful. The business partner contract must state that privacy protections continue after the contract ends, if there is a need for the business associate to retain any of the protected health information and for as long as the information is retained. In addition, the permissible uses of information after termination of the contract must be limited to those activities that make return or destruction of the information not feasible.

Comment: Many commenters recommended that providers and plans be excluded from the definition of ''business partner'' if they are already governed by the rule as covered entities. Providers expressed particular concern about the inclusion of physicians with hospital privileges as business partners of the hospital, as each hospital would

be required to have written contracts with and monitor the privacy practices of each physician with privileges, and each physician would be required to do the same for the hospital. Another commenter argued that consultations between covered entities for treatment or referral purposes should not be subject to the business partner contracting requirement.

Response: The final rule retains the general requirement that, subject to the exceptions below, a covered entity must enter into a business associate contract with another covered entity when one is providing services to or acting on behalf of the other. We retain this requirement because we believe that a covered entity that is a business associate should be restricted from using or disclosing the protected health information it creates or receives through its business associate function for any purposes other than those that are explicitly detailed in its contract.

However, the final rule expands the proposed exception for disclosures of protected health information by a covered health care provider to another health care provider. The final rule allows such disclosures without a business associate contract for any activities that fall under the definition of ''treatment.'' We agree with the commenter that the administrative burdens of requiring contracts in staff privileges arrangements would not be outweighed by any potential privacy enhancements from such a requirement. Although the exception for disclosure of protected health information for treatment could be sufficient to relieve physicians and hospitals of the contract requirement, we also believe that this arrangement does not meet the true meaning of ''business associate,'' because both the hospital and physician are providing services to the patient, not to each other. We therefore also add an exception to § 164.502(e)(1) that explicitly states that a contract is not required when the association involves a health care facility and another health care provider with privileges at that facility, if the purpose is providing health care to the individual. We have also added other exceptions in § 164.502(e)(1)(ii) to the requirement to obtain ''satisfactory assurances'' under § 164.502(e)(1)(i). We do not require a business associate arrangement between group health plans and their plan sponsors because other, albeit analogous, requirements apply under § 164.504(f) that are more tailored to the specifics of that legal relationship. We do not require business associate arrangements between government health plans providing public benefits and other agencies conducting certain functions for the health plan, because these arrangements are typically very constrained by other law.

Comment: Many commenters expressed concern that required contracts for federal agencies would adversely affect oversight activities, including investigations and audits. Some health plan commenters were concerned that if HMOs are business partners of an employer then the employer would have a right to all personal health information collected by the HMO. A commenter wanted to be sure that authorization would not be required for accreditation agencies to access information. A large manufacturing company wanted to make sure that business associate contracts were not required between affiliates and a parent corporation that provides administrative services for a sponsored health plan. Attorney commenters asserted that a business partner contract would undermine the attorney/client relationship, interfere with attorney/client privilege, and was not necessary to protect client confidences. A software vendor wanted to be excluded because the requirements for contracts were burdensome and government oversight intrusive. Some argued that because the primary purpose of medical device manufacturers is supplying devices, not patient care, they should be excluded.

Response: We clarify in the above discussion of the definition of ''business associate'' that a health insurance issuer or an HMO providing health insurance or health coverage to a group health plan does not become a business associate simply by providing health insurance or health coverage. The health insurance issuer or HMO may perform additional functions or activities or provide additional services, however, that would give rise to a business associate relationship. However, even when an health insurance issuer or HMO acts as a business associate of a group health plan, the group health plan has no right of access to the other protected health information maintained by the health insurance issuer or HMO. The business associate contract must constrain the uses and disclosures of protected health information obtained by the business associate through the relationship, but does not give the covered entity any right to request the business associate to disclose protected health information that it maintains outside of the business associate relationship to the group health plan. Under HIPAA, employers are not covered entities, so a health insurance issuer or HMO cannot act as a business associate of an employer. See § 164.504(f) with respect to disclosures to plan sponsors from a group health plan or health insurance issuer or HMO with respect to a group health plan.

With respect to attorneys generally, the reasons the commenters put forward to exempt attorneys from this requirement were not persuasive. The business associate requirements will not prevent attorneys from disclosing protected health information as necessary to find and prepare witness, nor from doing their work generally, because the business associate contract can allow disclosures for these purposes. We do not require business associate contracts to identify each disclosure to be made by the business associate; these disclosures can be identified by type or purpose. We believe covered entities and their attorneys can craft agreements that will allow for uses and disclosures of protected health information as necessary for these activities. The requirement for a business associate contract does not interfere with the attorney-client relationship, nor does it override professional judgement of business associates regarding the protected health information they need to discharge their responsibilities. We do not require covered entities to second guess their professional business associates' reasonable requests to use or disclose protected health information in the course of the relationship.

The attorney-client privilege covers only a small portion of information provided to attorneys and so is not a substitute for this requirement. More important, attorney-client privilege belongs to the client, in this case the covered entity, and not to the individual who is the subject of the information. The business associate requirements are intended to protect the subject of the information.

With regard to government attorneys and other government agencies, we recognize that federal and other law often does not allow standard legal contracts among governmental entities, but instead requires agreements to be made through the Economy Act or other mechanisms; these are generally reflected in a memorandum of understanding (MOU). We therefore modify the proposed requirements to allow government agencies to meet the required ''satisfactory assurance'' through such MOUs that contain the same provisions required of business associate contracts. As discussed elsewhere, we believe that direct regulation of entities receiving protected health information can be as or more effective in protecting health

information as contracts. We therefore also allow government agencies to meet the required ''satisfactory assurances'' if law or regulations impose requirements on business associates consistent with the requirements specified for business associate contracts.

We do not believe that the requirement to have a business associate contract with agencies that are performing the specified services for the covered entity or undertaking functions or activities on its behalf undermines the government functions being performed. A business associate arrangement requires the business associate to maintain the confidentiality of the protected health information and generally to use and disclose the information only for the purposes for which it was provided. This does not undermine government functions. We have exempted from the business associate requirement certain situations in which the law has created joint uses or custody over health information, such as when law requires another government agency to determine the eligibility for enrollment in a covered health plan. In such cases, information is generally shared across a number of government programs to determine eligibility, and often is jointly maintained. We also clarify that health oversight activities do not give rise to a business associate relationship, and that protected health information may be disclosed by a covered entity to a health oversight agency pursuant to § 164.512(d).

We clarify for purposes of the final rule that accreditation agencies are business associates of a covered entity and are explicitly included within the definition. During accreditation, covered entities disclose substantial amounts of protected health information to other private persons. A business associate contract basically requires the business associate to maintain the confidentiality of the protected health information that it receives and generally to use and disclose such information for the purposes for which it was provided. As with attorneys, we believe that requiring a business associate contract in this instance provides substantial additional privacy protection without interfering with the functions that are being provided by the business associate.

With regard to affiliates, § 164.504(d) permits affiliates to designate themselves as a single covered entity for purposes of this rule. (See § 164.504(d) for specific organizational requirements.) Affiliates that choose to designate themselves as a single covered entity for purposes of this rule will not need business associate contracts to share protected health information. Absent such designation, affiliates are business associates of the covered entity if they perform a function or service for the covered entity that necessitates the use or disclosure of protected health information.

Software vendors are business associates if they perform functions or activities on behalf of, or provide specified services to, a covered entity. The mere provision of software to a covered entity would not appear to give rise to a business associate relationship, although if the vendor needs access to the protected health information of the covered entity to assist with data management or to perform functions or activities on the covered entity's behalf, the vendor would be a business associate. We note that when an employee of a contractor, like a software or IT vendor, has his or her primary duty station on-site at a covered entity, the covered entity may choose to treat the employee of the vendor as a member of the covered entity's workforce, rather than as a business associate. See the preamble discussion to the definition of workforce, § 160.103.

With regard to medical device manufacturers, we clarify that a device manufacturer that provides ''health care'' consistent with the rule's definition, including being a ''supplier'' under the Medicare program, is a health care provider under the final rule. We do not require a business associate contract when protected health information is shared among health care providers for treatment purposes. However, a device manufacturer that does not provide ''health care'' must be a business associate of a covered entity if that manufacturer receives or creates protected health information in the performance of functions or activities on behalf of, or the provision of specified services to, a covered entity.

As to financial institutions, they are business associates under this rule when they conduct activities that cause them to meet the definition of business associate. See the preamble discussion of the definition of ''payment'' in § 164.501, for an explanation of activities of a financial institution that do not require it to have a business associated contract.

Disease managers may be health care providers or health plans, if they otherwise meet the respective definitions and perform disease management activities on their own behalf. However, such persons may also be business associates if they perform disease management functions or services for a covered entity.

Comment: Other commenters recommended that certain entities be included within the definition of ''business partner,'' such as transcription services; employee representatives; in vitro diagnostic manufacturers; private state and comparative health data organizations; state hospital associations; warehouses; ''whistleblowers,'' credit card companies that deal with health billing; and patients.

Response: We do not list all the types of entities that are business associates, because whether an entity is a business associate depends on what the entity does, not what the entity is. That is, this is a definition based on function; any entity performing the function described in the definition is a business associate. Using one of the commenters' examples, a state hospital association may be a business associate if it performs a service for a covered entity for which protected health information is required. It is not a business associate by virtue of the fact that it is a hospital association, but by virtue of the service it is performing.

Comment: A few commenters urged that certain entities, i.e., collection agencies and case managers, be business partners rather than covered entities for purposes of this rule.

Response: Collection agencies and case managers are business associates to the extent that they provide specified services to or perform functions or activities on behalf of a covered entity. A collection agency is not a covered entity for purposes of this rule. However, a case manager may be a covered entity because, depending on the case manager's activities, the person may meet the definition of either a health care provider or a health plan. See definitions of ''health care provider'' and ''health plan'' in § 164.501.

Comment: Several commenters complained that the proposed HIPAA security regulation and privacy regulation were inconsistent with regard to business partners.

Response: We will conform these policies in the final Security Rule.

Comment: One commenter expressed concern that the proposal appeared to give covered entities the power to limit by contract the ability of their business partners to disclose protected health information obtained from the covered entity regardless of whether the disclosure was permitted under proposed § 164.510, ''Uses and disclosures for which individual authorization is not required'' (§ 164.512 in the final rule). Therefore, the commenter argued that the covered

entity could prevent the business partner from disclosing protected health information to oversight agencies or law enforcement by omitting them from the authorized disclosures in the contract.

In addition, the commenter expressed concern that the proposal did not authorize business partners and their employees to engage in whistleblowing. The commenter concluded that this omission was unintended since the proposal's provision at proposed § 164.518(c)(4) relieved the covered entity, covered entity's employees, business partner, and the business partner's employees from liability for disclosing protected health information to law enforcement and to health oversight agencies when reporting improper activities, but failed to specifically authorize business partners and their employees to engage in whistleblowing in proposed § 164.510(f), ''Disclosures for law enforcement.''

Response: Under our statutory authority, we cannot directly regulate entities that are not covered entities; thus, we cannot regulate most business associates, or 'authorize' them to use or disclose protected health information. We agree with the result sought by the commenter, and accomplish it by ensuring that such whistle blowing disclosures by business associates and others do not constitute a violation of this rule on the part of the covered entity.

Comment: Some commenters suggested that the need to terminate contracts that had been breached would be particularly problematic when the contracts were with single-source business partners used by health care providers. For example, one commenter explained that when the Department awards single-source contracts, such as to a Medicare carrier acting as a fiscal intermediary that then becomes a business partner of a health care provider, the physician is left with no viable alternative if required to terminate the contract.

Response: In most cases, we expect that there will be other entities that could be retained by the covered entity as a business associate to carry out those functions on its behalf or provide the necessary services. We agree that under certain circumstances, however, it may not be possible for a covered entity to terminate a contract with a business associate. Accordingly, although the rule still generally requires a covered entity to terminate a contract if steps to cure such a material breach fail, it also allows an exception to this to accommodate those infrequent circumstances where there simply are no viable alternatives to continuing a contract with that particular business associate. It does not mean, however, that the covered entity can choose to continue the contract with a non-compliant business associate merely because it is more convenient or less costly than doing business with other potential business associates. We also require that if a covered entity determines that it is not feasible to terminate a non-compliant business associate, the covered entity must notify the Secretary.

Comment: Another commenter argued that having to renegotiate every existing contract within the 2-year implementation window so a covered entity can attest to ''satisfactory assurance'' that its business partner will appropriately safeguard protected health information is not practical.

Response: The 2-year implementation period is statutorily required under section 1175(b) of the Act. Further, we believe that two years provides adequate time to come into compliance with the regulation.

Comment: A commenter recommended that the business partner contract specifically address the issue of data mining because of its increasing prevalence within and outside the health care industry.

Response: We agree that protected health information should only be used by business associates for the purposes identified in the business associate contract. We address the issue of data mining by requiring that the business associate contract explicitly identify the uses or disclosures that the business associate is permitted to make with the protected health information. Aside from disclosures for data aggregation and business associate management, the business associate contract cannot authorize any uses or disclosures that the covered entity itself cannot make. Therefore, data mining by the business associate for any purpose not specified in the contract is a violation of the contract and grounds for termination of the contract by the covered entity.

Comment: One commenter stated that the rule needs to provide the ability to contract with persons and organizations to complete clinical studies, provide clinical expertise, and increase access to experts and quality of care.

Response: We agree, and do not prohibit covered entities from sharing protected health information under a business associate contract for these purposes.

Comment: A commenter requested clarification as to whether sister agencies are considered business partners when working together.

Response: It is unclear from the comment whether the ''sister agencies'' are components of a larger entity, are affiliated entities, or are otherwise linked. Requirements regarding sharing protected health information among affiliates and components are found in § 164.504.

Comment: One commenter stated that some union contracts specify that the employer and employees jointly conduct patient quality of care reviews. The commenter requested clarification as to whether this arrangement made the employee a business partner.

Response: An employee organization that agrees to perform quality assurance for a group health plan meets the definition of a business associate. We note that the employee representatives acting on behalf of the employee organization would be performing the functions of the organization, and the employee organization would be responsible under the business associate contract to ensure that the representatives abided by the restrictions and conditions of the contract. If the employee organization is a plan sponsor of the group health plan, the similar provisions of § 164.504(f) would apply instead of the business associate requirements. See § 164.502(e)(1).

Comment: Some commenters supported regulating employers as business partners of the health plan. These commenters believed that this approach provided flexibility by giving employers access to information when necessary while still holding employers accountable for improper use of the information. Many commenters, however, stressed that this approach would turn the relationship between employers, employees and other agents ''on its head'' by making the employer subordinate to its agents. In addition, several commenters objected to the business partner approach because they alleged it would place employers at risk for greater liability.

Response: We do not require a business associate contract for disclosure of protected health information from group health plans to employers. We do, however, put other conditions on the disclosure of protected health information from group health plans to employers who sponsor the plan. See further discussion in § 164.504 on disclosure of protected health information to employers.

Comment: One commenter expressed concern that the regulation would discourage organizations from participating with Planned Parenthood since pro bono and volunteer services may have no contract signed.

Response: We design the rule's requirements with respect to volunteers and pro bono services to allow flexibility to the covered entity so as not to disturb these arrangements. Specifically, when such volunteers work on the premises of the covered entity, the covered entity may choose to treat them as members of the covered entity's workforce or as business associates. See the definitions of business associate and workforce in § 160.103. If the volunteer performs its work off-site and needs protected health information, a business associate arrangement will be required. In this instance, where protected health information leaves the premises of the covered entity, privacy concerns are heightened and it is reasonable to require an agreement to protect the information. We believe that pro bono contractors will easily develop standard contracts to allow those activities to continue smoothly while protecting the health information that is shared.

Section 164.504(f)—Group Health Plans

Comment: Several commenters interpreted the preamble in the proposed rule to mean that only self-insured group health plans were covered entities. Another commenter suggested there was an error in the definition of group health plans because it only included plans with more than 50 participants *or* plans administered by an entity other than the employer (emphasis added by commenter). This commenter believed the ''or'' should be an ''and'' because almost all plans under 50 are administered by another entity and therefore this definition does not exclude most small plans.

Response: We did not intend to imply that only self-insured group health plans are covered health plans. We clarify that all group health plans, both self-insured and fully-funded, with 50 or more participants are covered entities, and that group health plans with fewer than 50 participants are covered health plans if they are administered by another entity. While we agree with the commenter that few group health plans with fewer than 50 participants are self-administered, the ''or'' is dictated by the statute. Therefore, the statute only exempts group health plans with fewer than 50 participants that are not administered by an entity other than the employer.

Comment: Several commenters stated that the proposed rule mis-characterized the relationship between the employer and the group health plan. The commenters stated that under ERISA and the Internal Revenue Code group health plans are separate legal entities from their employer sponsors. The group health plan itself, however, generally does not have any employees. Most operations of the group health plan are contracted out to other entities or are carried out by employees of the employer who sponsors the plan. The commenters stressed that while group health plans are clearly covered entities, the Department does not have the statutory authority to cover employers or other entities that sponsor group health plans. In contrast, many commenters stated that without covering employers, meaningful privacy protection is unattainable.

Response: We agree that group health plans are separate legal entities from their plan sponsors and that the group health plan itself may be operated by employees of the plan sponsor. We make significant modification to the proposed rule to better reflect this reality. We design the requirements in the final regulation to use the existing regulatory tools provided by ERISA, such as the plan documents required by that law and the constellation of plan administration functions defined by that law that established and maintain the group health plan.

We recognize plan sponsors' legitimate need for health information in certain situations while, at the same time, protecting health information from being used for employment-related functions or for other functions related to other employee benefit plans or other benefits provided by the plan sponsor. We do not attempt to directly regulate plan sponsors, but pursuant to our authority to regulate health plans, we place restrictions on the flow of information from covered entities to non-covered entities. The final rule permits group health plans to disclose protected health information to plan sponsors, and allows them to authorize health insurance issuers or HMOs to disclose protected health information to plan sponsors, if the plan sponsors agree to use and disclose the information only as permitted or required by the regulation. The information may be used only for plan administration functions performed on behalf of the group health plan and specified in the plan documents. Hereafter, any reference to employer in a response to a comment uses the term ''plan sponsor,'' since employers can only receive protected health information in their role as plan sponsors, except as otherwise permitted under this rule, such as with an authorization.

Specifically, in order for a plan sponsor to obtain without authorization protected health information from a group health plan, health insurance issuer, or HMO, the documents under which the group health plan was established and is maintained must be amended to: (1) Describe the permitted uses and disclosures of protected health information by the plan sponsor (see above for further explanation); (2) specify that disclosure is permitted only upon receipt of a written certification that the plan documents have been amended; and (3) provide adequate firewalls. The firewalls must identify the employees or classes of employees or other persons under the plan sponsor's control who will have access to protected health information; restrict access to only the employees identified and only for the administrative functions performed on behalf of the group health plan; and provide a mechanism for resolving issues of noncompliance by the employees identified. Any employee of the plan sponsor who receives protected health information in connection with the group health plan must be included in the amendment to the plan documents. As required by ERISA, the named fiduciary is responsible for ensuring the accuracy of amendments to the plan documents.

Group health plans, and health insurance issuers or HMOs with respect to the group health plan, that disclose protected health information to plan sponsors are bound by the minimum necessary standard as described in § 164.514.

Group health plans, to the extent they provide health benefits only through an insurance contract with a health insurance issuer or HMO and do not create, receive, or maintain protected health information (except for summary information or enrollment and disenrollment information), are not required to comply with the requirements of §§ 164.520 or 164.530, except for the documentation requirements of § 164.530(j). In addition, because the group health plan does not have access to protected health information, the requirements of §§ 164.524, 164.526, and 164.528 are not applicable. Individuals enrolled in a group health plan that provides benefits only through an insurance contract with a health insurance issuer or HMO would have access to all rights provided by this regulation through the health insurance issuer or HMO, because they are covered entities in their own right.

Comment: We received several comments from self-insured plans who stated that the proposed rule did not fully appreciate the dual nature of an employer as a plan sponsor and as a insurer. These commenters stated that

the regulation should have an exception for employers who are also insurers.

Response: We believe the approach we have taken in the final rule recognizes the special relationship between plan sponsors and group health plans, including group health plans that provide benefits through a self-insured arrangement. The final rule allows plan sponsors and employees of plan sponsors access to protected health information for purposes of plan administration. The group health plan is bound by the permitted uses and disclosures of the regulation, but may disclose protected health information to plan sponsors under certain circumstances. To the extent that group health plans do not provide health benefits through an insurance contract, they are required to establish a privacy officer and provide training to employees who have access to protected health information, as well as meet the other applicable requirements of the regulation.

Comment: Some commenters supported our position not to require individual consent for employers to have access to protected health information for purposes of treatment, payment, and health care operations. For employer sponsored insurance to continue to exist as it does today, the commenters stressed, this policy is essential. Other commenters encouraged the Department to amend the regulation to require authorization for disclosure of information to employers. These commenters stressed that because the employer was not a covered entity, individual consent is the only way to prohibit potential abuses of information.

Response: In the final regulation, we maintain the position in the proposed rule that a health plan, including a group health plan, need not obtain individual consent for use and disclosure of protected health information for treatment, payment and or health care operations purposes. However, we impose conditions (described above) for making such disclosures to the plan sponsor. Because employees of the plan sponsor often perform health care operations and payment (e.g. plan administration) functions, such as claims payment, quality review, and auditing, they may have legitimate need for such information. Requiring authorization from every participant in the plan could make such fundamental plan administration activities impossible. We therefore impose regulatory restrictions, rather than a consent requirement, to prevent abuses. For example, the plan sponsor must certify that any protected health information obtained by its employees through such plan administration activities will not be used for employment-related decisions.

Comment: Several commenters stressed that the regulation must require the establishment of firewalls between group health plans and employers. These commenters stated that firewalls were necessary to prevent the employer from accessing information improperly and using it in making job placements, promotions, and firing decisions. In addition, one commenter stated that employees with access to protected health information must be empowered through this regulation to deny unauthorized access to protected health information to corporate managers and executives.

Response: We agree with the commenters that firewalls are necessary to prevent unauthorized use and disclosure of protected health information. Among the conditions for group health plans to disclose information to plan sponsors, the plan sponsor must establish firewalls to prevent unauthorized uses and disclosures of information. The firewalls include: describing the employees or classes of employees with access to protected health information; restricting access to and use of the protected health information to the plan administration functions performed on behalf of the group health plan and described in plan documents; and providing an effective mechanism for resolving issues of noncompliance.

Comment: Several commenters supported our proposal to cover the health care component of an employer in its capacity as an administrator of the group health plan. These commenters felt the component approach was necessary to prevent the disclosure of protected health information to other parts of the employer where it might be used or disclosed improperly. Other commenters believed the component approach was unworkable and that distinguishing who was in the covered entity would not be as easy as assumed in the proposed rule. One commenter stated it was unreasonable for an employer to go through its workforce division by division and employee by employee designating who is included in the component and who is not. In addition, some commenters argued that we did not have the statutory authority to regulate employers at all, including their health care components.

One commenter requested more guidance with respect to identifying the health care component as proposed under the proposed rule. In particular, the commenter requested that the regulation clearly define how to identify such persons and what activities and functional areas may be included. The commenter alleged that identification of persons needing access to protected health information will be administratively burdensome. Another commenter requested clarification on distinguishing the component entity from non-component entities within an organization and how to administer such relationships. The commenter stated that individuals included in the covered entity could change on a daily basis and advocated for a simpler set of rules governing intra-organizational relationships as opposed to inter-organizational relationships.

Response: While we have not adopted the component approach for plan sponsors in the final rule, plan sponsors who want protected health information must still identify who in the organization will have access to the information. Several of the changes we make to the NPRM will make this designation easier. First, we move from ''component'' to a more familiar functional approach. We limit the employees of the plan sponsor who may receive protected health information to those employees performing plan administration functions, as that term is understood with respect to ERISA compliance, and as limited by this rule's definitions of payment and health care operation. We also allow designation of a class of employees (e.g., all employees assigned to a particular department) or individual employees.

Although some commenters have asked for guidance, we have intentionally left the process flexible to accommodate different organizational structures. Plan sponsors may identify who will have access to protected health information in whatever way best reflects their business needs as long as participants can reasonably identify who will have access. For example, persons may be identified by naming individuals, job titles (e.g. Director of Human Resources), functions (e.g. employees with oversight responsibility for the outside third party claims administrator), divisions of the company (e.g. Employee Benefits) or other entities related to the plan sponsor. We believe this flexibility will also ease any administrative burden that may result from the identification process. Identification in terms such as ''individuals who from time to time may need access to protected health information'' or in other broad or generic ways, however, would not be sufficient.

Comment: In addition to the comments on the component approach itself, several commenters pointed out

that many employees wear two hats in the organization, one for the group health plan and one for the employer. The commenters stressed that these employees should not be regulated when they are performing group health plan functions. This arrangement is necessary, particularly in small employers where the plan fiduciary may also be in charge of other human resources functions. The commenter recommended that employees be allowed access to information when necessary to perform health plan functions while prohibiting them from using the information for non-health plan functions.

Response: We agree with the commenters that many employees perform multiple functions in an organization and we design these provisions specifically to accommodate this way of conducting business. Under the approach taken in the final regulation, employees who perform multiple functions (i.e. group health plan and employment-related functions) may receive protected health information from group health plans, but among other things, the plan documents must certify that these employees will not use the information for activities not otherwise permitted by this rule including for employment-related activities.

Comment: Several commenters pointed out that the amount of access needed to protected health information varies greatly from employer to employer. Some employers may perform many plan administration functions themselves which are not possible without access to protected health information. Other employers may simply offer health insurance by paying a premium to a health insurance issuer rather than provide or administer health benefits themselves. Some commenters argued that fully insured plans should not be covered under the rule. Similarly, some commenters argued that the regulation was overly burdensome on small employers, most of whom fully insure their group health plans. Other commenters pointed out that health insurance issuers—even in fully insured arrangements—are often asked for identifiable health information, sometimes for legitimate purposes such as auditing or quality assurance, but sometimes not. One commenter, representing an insurer, gave several examples of employer requests, including claims reports for employees, individual and aggregate amounts paid for employees, identity of employees using certain drugs, and the identity, diagnosis and anticipated future costs for ''high cost'' employees. This same commenter requested guidance in what types of information can be released to employers to help them determine the organization's responsibilities and liabilities.

Response: In the final regulation we recognize the diversity in plan sponsors' need for protected health information. Many plan sponsors need access to protected health information to perform plan administration functions, including eligibility and enrollment functions, quality assurance, claims processing, auditing, monitoring, trend analysis, and management of carve-out plans (such as vision and dental plans). In the final regulation we allow group health plans to disclose protected health information to plan sponsors if the plan sponsor voluntarily agrees to use the information only in accordance with the purposes stated in the plan documents and as permitted by the regulation. We clarify, however, that plan administration does not include any employment-related decisions, including fitness for duty determinations, or duties related to other employee benefits or plans. Plan documents may only permit health insurance issuers to disclose protected health information to a plan sponsor as is otherwise permitted under this rule and consistent with the minimum necessary standard.

Some plan sponsors, including those with a fully insured group health plan, do not perform plan administration functions on behalf of group health plans, but still may require health information for other purposes, such as modifying, amending or terminating the plan or soliciting bids from prospective issuers or HMOs. In the ERISA context actions undertaken to modify, amend or terminate a group health plan may be known as ''settlor'' functions (see *Lockheed Corp.* v. *Spink,* 517 U.S. 882 (1996)). For example, a plan sponsor may require access to information to evaluate whether to adopt a three-tiered drug formulary. Additionally, a prospective health insurance issuer may need claims information from a plan sponsor in order to provide rating information. The final rule permits plan sponsors to receive summary health information with identifiers removed in order to carry out such functions. Summary health information is information that summarizes the claims history, expenses, or types of claims by individuals enrolled in the group health plan. In addition, the identifiers listed in § 164.514(b)(2)(i) must be removed prior to disclosing the information to a plan sponsor for purposes of modifying, amending, or terminating the plan. See § 164.504(a). This information does not constitute de-identified information because there may be a reasonable basis to believe the information is identifiable to the plan sponsor, especially if the number of participants in the group health plan is small. A group health plan, however, may not permit an issuer or HMO to disclose protected health information to a plan sponsor unless the requirement in § 164.520 states that this disclosure may occur.

Comment: Several commenters stated that health insurance issuers cannot be held responsible for employers' use of protected health information. They stated that the issuer is the agent of the employer and it should not be required to monitor the employer's use and disclosure of information.

Response: Under this regulation, health insurance issuers are covered entities and responsible for their own uses and disclosures of protected health information. A group health plan must require a health insurance issuer or HMO providing coverage to the group health plan to disclose information to the plan sponsor only as provided in the plan documents.

Comment: Several commenters urged us to require de-identified information to be used to the greatest extent possible when information is being shared with employers.

Response: De-identified information is not sufficient for many functions plan sponsors perform on behalf of their group health plans. We have created a process to allow plan sponsors and their employees access to protected health information when necessary to administer the plan. We note that all uses and disclosures of protected health information by the group health plan are bound by the minimum necessary standard.

Comment: One commenter representing church plans argued that the regulation should treat such plans differently from other group health plans. The commenter was concerned about the level of access to information the Secretary would have in performing compliance reviews and suggested that a higher degree of sensitivity is need for information related to church plans than information related to other group health plans. This sensitivity is needed, the commenter alleged, to reduce unnecessary intrusion into church operations. The commenter also advocated that church plans found to be out of compliance should be able to self-correct within a stated time frame (270 days) and avoid paying penalty taxes as allowed in the Internal Revenue Code.

Response: We do not believe there is sufficient reason to treat church plans differently than other covered entities.

The intent of the compliance reviews is to determine whether or not the plan is abiding by the regulation, not to gather information on the general operations of the church. As required by § 160.310(c), the covered entity must provide access only to information that is pertinent to ascertaining compliance with part 160 or subpart E of 164.

Comment: Several commenters stated that employers often advocate on behalf of their employees in benefit disputes and appeals, answer questions with regard to the health plan, and generally help them navigate their health benefits. These commenters questioned whether this type of assistance would be allowed under the regulation, whether individual consent was required, and whether this intervention would make them a covered entity.

Response: The final rule does nothing to hinder or prohibit plan sponsors from advocating on behalf of group health plan participants or providing assistance in understanding their health plan. Under the privacy rule, however, the plan sponsor could not obtain any information from the group health plan or a covered provider unless authorization was given. We do not believe obtaining authorization when advocating or providing assistance will be impractical or burdensome since the individual is requesting assistance and therefore should be willing to provide authorization. Advocating on behalf of participants or providing other assistance does not make the plan sponsor a covered entity.

Section 164.506—Consent for Treatment, Payment, and Health Care Operations

Comment: Many commenters supported regulatory authorization for treatment, payment, and health care operations. In particular, health plans, employers, and institutional providers supported the use of regulatory authorization for treatment, payment, and health care operations.

In contrast, a large number of commenters, particularly health care professionals, patients, and patient advocates, suggested that consent for treatment, payment, and health care operations should be required. Many commenters supported the use of consent for treatment, payment, and health care operations, considering this a requirement for maintaining the integrity of the health care system. Some commenters made a distinction between requiring and permitting providers to obtain consent.

Commenters nearly uniformly agreed that covered health care providers, health plans, and clearinghouses should not be prohibited from seeking authorization for treatment, payment, and health care operations. Some commenters stated that the prohibition against obtaining an authorization goes against professional ethics, undermines the patient-provider relationship, and is contrary to current industry practice.

Some commenters specifically noted the primacy of the doctor-patient relationship regarding consent. In general, commenters recommended that individually identifiable health information not be released by doctors without patient consent. A few commenters stated that prohibiting health care providers from obtaining consent could cause the patient to become suspicious and distrustful of the health care provider. Other commenters believed that clinicians have the responsibility for making sure that patients are fully informed about the consequences of releasing information. A few commented that the process of obtaining consent provided an opportunity for the patient and provider to negotiate the use and disclosure of patient information.

Commenters discussed how, when, and by whom consent should be sought. For example, some commenters viewed a visit between a health care provider and patient as the appropriate place for consent to be discussed and obtained. While others did not necessarily dispute the appropriateness of health care providers obtaining consent for uses and disclosures of protected health information from individuals, some said that it was appropriate for health plans to be permitted to obtain consent.

Response: In the NPRM we stated our concern that the blanket consents that individuals sign today provide these individuals with neither notice nor control over how their information is to be used. While we retain those concerns, we also understand that for many who participate in the health care system, the acts of providing and obtaining consent represent important values that these parties wish to retain. Many individuals argued that providing consent enhances their control; many advocates argued that the act of consent focuses patient attention on the transaction; and many health care providers argued that obtaining consent is part of ethical behavior.

The final rule amends our proposed approach and requires most covered health care providers to obtain a consent from their patients to use or disclose protected health information for treatment, payment, and health care operations. Providers who have an indirect treatment relationship with the patient, as defined in § 164.501, cannot be expected to have an opportunity to obtain consent and may continue to rely on regulatory authorization for their uses and disclosures for these purposes.

As described in the comments, it is the relationship between the health care provider and the patient that is the basis for many decisions about uses and disclosures of protected health information. Much of the individually identifiable health information that is the subject of this rule is created when a patient interacts with a health care provider. By requiring covered providers to obtain consent for treatment, payment, and health care operations, the individual will have appropriate opportunity to consider the appropriate uses and disclosures of his or her protected health information. We also require that the consent contain a reference to the provider's notice, which contains a more detailed description of the provider's practices relating to uses and disclosures of protected health information. This combination provides the basis for an individual to have an informed conversation with his or her provider and to request restrictions.

It is our understanding that it is common practice for providers to obtain consent for this type of information-sharing today. Many providers and provider organizations stated that they are ethically obligated to obtain the patient's consent and that it is their practice to do so. A 1998 study by Merz, et al, published in the Journal of Law, Medicine and Ethics examined hospital consent forms regarding disclosure of medical information.[8] They found that 97% of all hospitals seek consent for the release of information for payment purposes; 45% seek consent for disclosure for utilization review, peer review, quality assurance, and/or prospective review; and 50% seek consent for disclosure to providers, other health care facilities, or others for continuity of care purposes. All of these activities fall within our definitions of treatment, payment, or health care operations.

In the final rule we have not required that health plans or health care clearinghouses obtain consent for their uses and disclosures of protected health information for treatment, payment, or health care operations. The rationale underlying the consent requirements for uses and disclosures by health care providers do not pertain to health plans and health care clearinghouses. First, current practice is varied, and there is little history of health plans obtaining

[8] J. Merz, P. Sankar, S.S. Yoo, ''Hospital Consent for Disclosure of Medical Records,'' Journal of Law, Medicine & Ethics, 26 (1998): 241–248.

consent relating to their own information practices unless required to do so by some other law. This is reflected in the public comments, in which most health plans supported the regulatory authorization approach proposed in the NPRM. Further, unlike many health care providers, health plans did not maintain that they were ethically obligated to seek the consent of their patients for their use and disclosure activities. Finally, it is the unique relationship between an individual and his or her health care provider that provides the foundation for a meaningful consent process. Requiring that consent process between an individual and a health plan or clearinghouse, when no such unique relationship exists, we believe is not necessary.

Unlike their relationship with health care providers, individuals in most instances do not have a direct opportunity to engage in a discussion with a health plan or clearinghouse at the time that they enter into a relationship with those entities. Most individuals choose a health plan through their employer and often sign up through their employer without any direct contact with the health plan. We concluded that providing for a signed consent in such a circumstance would add little to the proposed approach, which would have required health plans to provide a detailed notice to their enrollees. In the final rule, we also clarify that an individual can request a restriction from a health plan or health care clearinghouse. Since individuals rarely if ever have any direct contact with clearinghouses, we concluded that requiring a signed consent would have virtually no effect beyond the provision of the notice and the opportunity to request restrictions.

We agree with the comments we received objecting to the provision prohibiting covered entities from obtaining consent from individuals. As discussed above, in the final rule we require covered health care providers with direct treatment relationships to obtain consent to use or disclose protected health information for treatment, payment, and health care operations. In addition, we have eliminated the provision prohibiting other covered entities from obtaining such consents. We note that the consents that covered entities are permitted to obtain relate to their own uses and disclosures of protected health information for treatment, payment, and health care operations and not to the practices of others. If a covered entity wants to obtain the individual's permission to receive protected health information from another covered entity, it must do so using an authorization under § 164.508.

''Consent'' versus ''Authorization''

Comment: In general, commenters did not distinguish between ''consent'' and ''authorization.'' Commenters used both terms to refer to the individual's giving permission for the use and disclosure of protected health information by any entity.

Response: In the final rule we have made an important distinction between consent and authorization. Under the final rule, we refer to the process by which a covered entity seeks agreement from an individual regarding how it will use and disclose the individual's protected health information for treatment, payment, and health care operations as ''consent.'' The provisions in the final rule relating to consent are largely contained in § 164.506. The process by which a covered entity seeks agreement from an individual to use or disclose protected health information for other purposes, or to authorize another covered entity to disclose protected health information to the requesting covered entity, are termed ''authorizations'' and the provisions relating to them are found in § 164.508.

Consent Requirements

Comment: Many commenters believed that consent might be problematic in that it could allow covered entities to refuse enrollment or services if the individual does not grant the consent. Some commenters proposed that covered entities be allowed to condition treatment, payment, or health care operations on whether or not an individual granted consent. Other commenters said that consent should be voluntary and not coerced.

Response: In the final rule (§ 164.506(b)(1)), we permit covered health care providers to condition treatment on the individual's consent to the covered provider's use or disclosure of protected health information to carry out treatment, payment, and health care operations. We recognize that it would be difficult, if not impossible, for health care providers to treat their patients and run their businesses without being able to use or disclose protected health information for these purposes. For example, a health care provider could not be reimbursed by a health plan unless the provider could share protected health information about the individual with the health plan. Under the final rule, if the individual refuses to grant consent for this disclosure, the health care provider may refuse to treat the individual. We encourage health care providers to exhaust other options, such as making alternative payment arrangements with the individual, before refusing to treat the individual on these grounds.

We also permit health plans to condition enrollment in the health plan on the individual's consent for the health plan to use and disclose protected health information to carry out treatment, payment, and health care operations (see § 164.506(b)(2)). The health plan must seek the consent in conjunction with the individual's enrollment in the plan for this provision to apply. For example, a health plan's application for enrollment may include a consent for the health plan to use or disclose protected health information to carry out treatment, payment, and/or health care operations. If the individual does not sign this consent, the health plan, under § 164.502(a)(1)(iii), is prohibited from using or disclosing protected health information about the individual for the purposes stated in the consent form. Because the health plan may not be able adequately to provide services to the individual without these uses and disclosures, we permit the health plan to refuse to enroll the individual if the consent is not signed.

Comment: Some commenters were concerned that the NPRM conflicted with state law regarding when covered entities would be required to obtain consent for uses and disclosures of protected health information.

Response: We have modified the provisions in the final rule to require certain health care providers to obtain consent for uses and disclosures for treatment, payment, and health care operations and to permit other covered entities to do so. A consent under this rule may be combined with other types of written legal permission from the individual, such as state-required consents for uses and disclosures of certain types of health information (e.g., information relating to HIV/AIDS or mental health). We also permit covered entities to seek authorization from the individual for another covered entity's use or disclosure of protected health information for these purposes, including if the covered entity is required to do so by other law. Though we do not believe any states currently require such authorizations, we wanted to avoid future conflicts. These changes should resolve the concerns raised by commenters regarding conflicts with state laws that require consent, authorization, or other types of written legal permission for uses and disclosures of protected health information.

Comment: Some commenters noted that there would be circumstances when consent is impossible or impractical. A few commenters suggested that in such situations patient information be de-identified or reviewed by an objective third party to determine if consent is necessary.

Response: Covered health care providers with direct treatment relationships are required to obtain consent to use or disclose protected health information to carry out treatment, payment, and health care operations. In certain treatment situations where the provider is permitted or required to treat an individual without the individual's written consent to receive health care, the provider may use and disclose protected health information created or obtained in the course of that treatment without the individual's consent under this rule (see § 164.506(a)(3)). In these situations, the provider must attempt to obtain the individual's consent and, if the provider is unable to obtain consent, the provider must document the attempt and the reason consent could not be obtained. Together with the uses and disclosures permitted under §§ 164.510 and 164.512, the concerns raised regarding situations in which it is impossible or impractical for covered entities to obtain the individual's permission to use or disclose protected health information about the individual have been addressed.

Comment: An agency that provides care to individuals with mental retardation and developmental disabilities expressed concern that many of their consumers lack capacity to consent to the release of their records and may not have a surrogate readily available to provide consent on their behalf.

Response: Under § 164.506(a)(3), we provide exceptions to the consent requirement for certain treatment situations in which consent is difficult to obtain. In these situations, the covered provider must attempt to obtain consent and must document the reason why consent was not obtained. If these conditions are met, the provider may use and disclose the protected health information created or obtained during the treatment for treatment, payment, or health care operations purposes, without consent.

Comment: Many commenters were concerned that covered entities working together in an integrated health care system would each separately be required to obtain consent for use and disclosure of protected health information for treatment, payment, and health care operations. These commenters recommend that the rule permit covered entities that are part of the same integrated health care system to obtain a single consent allowing each of the covered entities to use and disclose protected health information in accordance with that consent form. Some commenters said that it would be confusing to patients and administratively burdensome to require separate consents for health care systems that include multiple covered entities.

Response: We agree with commenters' concerns. In § 164.506(f) of the final rule we permit covered entities that participate in an organized health care arrangement to obtain a single consent on behalf of the arrangement. See § 164.501 and the corresponding preamble discussion regarding organized health care arrangements. To obtain a joint consent, the covered entities must have a joint notice and must refer to the joint notice in the joint consent. See § 164.520(d) and the corresponding preamble discussion regarding joint notice. The joint consent must also identify the covered entities to which it applies so that individuals will know who is permitted to use and disclose information about them.

Comment: Many commenters stated that individuals own their medical records and, therefore, should have absolute control over them, including knowing by whom and for what purpose protected health information is used, disclosed, and maintained. Some commenters asserted that, according to existing law, a patient owns the medical records of which he is the subject.

Response: We disagree. In order to assert an ownership interest in a medical record, a patient must demonstrate some legitimate claim of entitlement to it under a state law that establishes property rights or under state contract law. Historically, medical records have been the property of the health care provider or medical facility that created them, and some state statutes directly provide that medical records are the property of a health care provider or a health care facility. The final rule is consistent with current state law that provides patients access to protected health information but not ownership of medical records. Furthermore, state laws that are more stringent than the rule, that is, state laws that provide a patient with greater access to protected health information, remain in effect. See discussion of ''Preemption'' above.

Electronically Stored Data

Comment: Some commenters stated that privacy concerns would be significantly reduced if patient information is not stored electronically. One commenter suggested that consent should be given for patient information to be stored electronically. One commenter believed that information stored in data systems should not be individually identifiable.

Response: We agree that storing and transmitting health information electronically creates concerns about the privacy of health information. We do not agree, however, that covered entities should be expected to maintain health information outside of an electronic system, particularly as health care providers and health plans extend their reliance on electronic transactions. We do not believe that it would be feasible to permit individuals to opt out of electronic transactions by withholding their consent. We note that individuals can ask providers and health plans whether or not they store information electronically, and can choose only providers who do not do so or who agree not to do so. We also do not believe that it is practical or efficient to require that electronic data bases contain only de-identified information. Electronic transactions have achieved tremendous savings in the health care system and electronic records have enabled significant improvements in the quality and coordination of health care. These improvements would not be possible with de-identified information.

Section 164.508—Uses and Disclosures for Which Authorization Is Required

Uses and Disclosures Requiring Authorization

Comment: We received many comments in general support of requiring authorization for the use or disclosure of protected health information. Some comments suggested, however, that we should define those uses and disclosures for which authorization is required and permit covered entities to make all other uses and disclosures without authorization.

Response: We retain the requirement for covered entities to obtain authorization for all uses and disclosures of protected health information that are not otherwise permitted or required under the rule without authorization. We define exceptions to the general rule requiring authorization for the use or disclosure of protected health information, rather than defining narrow circumstances in which authorization is required.

We believe this approach is consistent with well-established privacy principles, with other law, and with industry standards and ethical

guidelines. The July 1977 Report of the Privacy Protection Study Commission recommended that ''each medical-care provider be considered to owe a duty of confidentiality to any individual who is the subject of a medical record it maintains, and that, therefore, no medical care provider should disclose, or be required to disclose, in individually identifiable form, any information about any such individual without the individual's explicit authorization, unless the disclosures would be'' for specifically enumerated purposes such as treatment, audit or evaluation, research, public health, and law enforcement.[9] The Commission made similar recommendations with respect to insurance institutions.[10] The Privacy Act (5 U.S.C. 552a) prohibits government agencies from disclosing records except pursuant to the written request of or pursuant to a written consent of the individual to whom the record pertains, unless the disclosure is for certain specified purposes. The National Association of Insurance Commissioners' Health Information Privacy Model Act states, ''A carrier shall not collect, use or disclose protected health information without a valid authorization from the subject of the protected health information, except as permitted by * * * this Act or as permitted or required by law or court order. Authorization for the disclosure of protected health information may be obtained for any purpose, provided that the authorization meets the requirements of this section.'' In its report ''Best Principles for Health Privacy,'' the Health Privacy Working Group stated, ''Personally identifiable health information should not be disclosed without patient authorization, except in limited circumstances' such as when required by law, for oversight, and for research.[11] The American Medical Association's Council on Ethical and Judicial Affairs has issued an opinion stating, ''The physician should not reveal confidential communications or information without the express consent of the patient, unless required to do so by law [and] subject to certain exceptions which are ethically and legally justified because of overriding social considerations.'' [12] We build on these standards in this final rule.

Comment: Some comments suggested that, under the proposed rule, a covered entity could not use protected health information to solicit authorizations from individuals. For example, a covered entity could not use protected health information to generate a mailing list for sending an authorization for marketing purposes.

Response: We agree with this concern and clarify that covered entities are permitted to use protected health information in this manner without authorization as part of the management activities relating to implementation of and compliance with the requirements of this rule. See § 164.501 and the corresponding preamble regarding the definition of health care operations.

Comment: We received several comments suggesting that we not require written authorizations for disclosures to the individual or for disclosures initiated by the individual or the individual's legal representative.

Response: We agree with this concern and in the final rule we clarify that disclosures of protected health information to the individual who is the subject of the information do not require the individual's authorization. See § 164.502(a)(1). We do not intend to impose barriers between individuals and disclosures of protected health information to them.

When an individual requests that the covered entity disclose protected health information to a third party, however, the covered entity must obtain the individual's authorization, unless the third party is a personal representative of the individual with respect to such protected health information. See § 164.502(g). If under applicable law a person has authority to act on behalf of an individual in making decisions related to health care, except under limited circumstances, that person must be treated as the personal representative under this rule with respect to protected health information related to such representation. A legal representative is a personal representative under this rule if, under applicable law, such person is able to act on behalf of an individual in making decisions related to health care, with respect to the protected health information related to such decisions. For example, an attorney of an individual may or may not be a personal representative under the rule depending on the attorney's authority to act on behalf of the individual in decisions related to health care. If the attorney is the personal representative under the rule, he may obtain a copy of the protected health information relevant to such personal representation under the individual's right to access. If the attorney is not the personal representative under the rule, or if the attorney wants a copy of more protected health information than that which is relevant to his personal representation, the individual would have to authorize such disclosure.

Comment: Commenters expressed concern about whether a covered entity can rely on authorizations made by parents on behalf of their minor children once the child has reached the age of majority and recommended that covered entities be able to rely on the most recent, valid authorization, whether it was authorized by the parent or the minor.

Response: We agree. If an authorization is signed by a parent, who is the personal representative of the minor child at the time the authorization is signed, the covered entity may rely on the authorization for as long as it is a valid authorization, in accordance with § 164.508(b). A valid authorization remains valid until it expires or is revoked. This protects a covered entity's reasonable reliance on such authorization. The expiration date of the authorization may be the date the minor will reach the age of majority. In that case, the covered entity would be required to have the individual sign a new authorization form in order to use or disclose information covered in the expired authorization form.

Comment: Some commenters were concerned that covered entities working together in an integrated system would each be required to obtain authorization separately. These commenters suggested the rule should allow covered entities that are part of the same system to obtain a single authorization allowing each of the covered entities to use and disclose protected health information in accordance with that authorization.

Response: If the rule does not permit or require a covered entity to use or disclose protected health information without the individual's authorization, the covered entity must obtain the individual's authorization to make the use or disclosure. Multiple covered entities working together as an integrated delivery system or otherwise may satisfy this requirement in at least three ways. First, each covered entity may separately obtain an authorization directly from the individual who is the subject of the protected health information to be used or disclosed. Second, one covered entity may obtain

[9] Privacy Protection Study Commission, ''Personal Privacy in an Information Society,'' July 1977, p. 306.

[10] Privacy Protection Study Commission, ''Personal Privacy in an Information Society,'' July 1977, pp. 215–217.

[11] Health Privacy Working Group, ''Best Principles for Health Privacy,'' Health Privacy Project, Institute for Health Care Research and Policy, Georgetown University, July 1999, p. 19.

[12] AMA Council on Ethical and Judicial Affairs, ''Opinion E–5.05: Confidentiality,'' Issued December 1983, Updated June 1994.

a compound authorization in accordance with § 164.508(b)(3) that authorizes multiple covered entities to use and disclose protected health information. In accordance with § 164.508(c)(1)(ii), each covered entity, or class of covered entities, that is authorized to make the use or disclosure must be clearly identified. Third, if the requirements in § 164.504(d) are met, the integrated delivery system may elect to designate itself as a single affiliated covered entity. A valid authorization obtained by that single affiliated covered entity would satisfy the authorization requirements for each covered entity within the affiliated covered entity. Whichever option is used, because these authorizations are being requested by a covered entity for its own use or disclosure, the authorization must contain both the core elements in § 164.508(c) and the additional elements in § 164.508(d).

Sale, Rental, or Barter

Comment: Proposed § 164.508 listed examples of activities that would have required authorization, which included disclosure by sale, rental, or barter. Some commenters requested clarification that this provision is not intended to affect mergers, sale, or similar transactions dealing with entire companies or their individual divisions. A few commenters stated that covered entities should be allowed to sell protected health information, including claims data, as an asset of the covered entity.

Response: We clarify in the definition of health care operations that a covered entity may sell or transfer its assets, including protected health information, to a successor in interest that is or will become a covered entity. See § 164.501 and the corresponding preamble discussion regarding this change. We believe this change meets commenters' business needs without compromising individuals' privacy interests.

Comment: Some commenters supported the requirement for covered entities to obtain authorization for the sale, rental, or barter of protected health information. Some commenters argued that protected health information should never be bought or sold by anyone, even with the individual's authorization.

Response: We removed the reference to sale, rental, or barter in the final rule because we determined that the term was overly broad. For example, if a researcher reimbursed a provider for the cost of configuring health data to be disclosed under the research provisions at § 164.512(i), there may have been ambiguity that this was a sale and, therefore, required authorizations from the individuals who were the subjects of the information. We clarify in the final rule that if the use or disclosure is otherwise permitted or required under the rule without authorization, such authorization is not required simply because the disclosure is made by sale, rental, or barter.

Comment: Many commenters expressed concerns that their health information will be sold to pharmaceutical companies.

Response: Although we have removed the reference to sale, rental or barter, the final rule generally would not permit the sale of protected health information to a pharmaceutical company without the authorization of individuals who are the subjects of the information. In some cases, a covered entity could disclose protected health information to a pharmaceutical company for research purposes if the disclosure met the requirements of § 164.512(i).

Psychotherapy Notes

Comment: Public response to the concept of providing additional protections for psychotherapy notes was divided. Many individuals and most providers, particularly mental health practitioners, advocated requiring consent for use or disclosure of all or most protected health information, but particularly sensitive information such as mental health information, not necessarily limited to psychotherapy notes. Others thought there should be special protections for psychotherapy information based on the federal psychotherapist-patient privilege created by the U.S. Supreme Court in *Jaffee* v. *Redmond* and the need for an atmosphere of trust between therapist and patient that is required for effective psychotherapy. Several consumer groups recommended prohibiting disclosure of psychotherapy notes for payment purposes.

Some commenters, however, saw no need for special protections for psychotherapy communications and thought that the rules should apply the same protections for all individually identifiable information. Other commenters who advocated for no special protections based their opposition on the difficulty in drawing a distinction between physical and mental health and that special protections should be left to the states. Many health plans and employers did not support additional protections for psychotherapy notes because they stated they need access to this information to assess the adequacy of treatment, the severity of a patient's condition, the extent of a disability, or the ability to monitor the effectiveness of an individual's mental health care and eligibility for benefits. Other commenters, many from insurance companies, cited the need to have psychotherapy notes to detect fraud.

A few commenters said that it was not necessary to provide additional protections to psychotherapy notes because the ''minimum necessary'' provisions of the NPRM provide sufficient protections.

Response: In the final rule, a covered entity generally must obtain an authorization for disclosure of psychotherapy notes, or for use by a person other than the person who created the psychotherapy notes. This authorization is specific to psychotherapy notes and is in addition to the consent an individual may have given for the use or disclosure of other protected health information to carry out treatment, payment, and health care operations. This additional level of individual control provides greater protection than a general application of the ''minimum necessary'' rule. Nothing in this regulation weakens existing rules applicable to mental health information that provide more stringent protections. We do not intend to alter the holding in *Jaffee* v. *Redmond.*

Generally, we have not treated sensitive information differently from other protected health information; however, we have provided additional protections for psychotherapy notes because of *Jaffee* v. *Redmond* and the unique role of this type of information. There are few reasons why other health care entities should need access to psychotherapy notes, and in those cases, the individual is in the best position to determine if the notes should be disclosed. As we have defined them, psychotherapy notes are primarily of use to the mental health professional who wrote them, maintained separately from the medical record, and not involved in the documentation necessary to carry out treatment, payment, or health care operations. Since psychotherapy notes have been defined to exclude information that health plans would typically need to process a claim for benefits, special authorization for payment purposes should be rare. Unlike information shared with other health care providers for the purposes of treatment, psychotherapy notes are more detailed and subjective and are today subject to unique privacy and record retention practices. In fact, it is this separate existence and isolated use that allows us to grant the extra protection without causing an undue burden on the health care system.

Comment: Many commenters suggested we prohibit disclosure of psychotherapy notes without authorization for uses and disclosures under proposed § 164.510 of the NPRM, or that protections should be extended to particular uses and disclosures, such as disclosures for public health, law enforcement, health oversight, and judicial and administrative proceedings. One of these commenters stated that the only purpose for which psychotherapy notes should be disclosed without authorization is for preventing or lessening a serious or imminent threat to health or safety (proposed § 154.510(k)). Another commenter stated that the rule should allow disclosure of psychotherapy notes without authorization for this purpose, or as required by law in cases of abuse or neglect.

Other commenters did not want these protections to be extended to certain national priority activities. They claimed that information relative to psychotherapy is essential to states' activities to protect the public from dangerous mentally ill offenders and abusers, to deliver services to individuals who are unable to authorize release of health care information, and for public health assessments. One commenter requested clarification of when psychotherapy notes could be released in emergency circumstances. Several commenters stated that psychotherapy notes should not be disclosed for public health purposes.

Response: We agree with the commenters who suggested extending protections of psychotherapy notes and have limited the purposes for which psychotherapy notes may be disclosed without authorization for purposes other than treatment, payment, or health care operations. The final rule requires covered entities to obtain authorization to use or disclose psychotherapy notes for purposes listed in § 164.512, with the following exceptions: An authorization is not required for use or disclosure of psychotherapy notes when the use or disclosure is required for enforcement of this rule, in accordance with § 164.502(a)(2)(ii); when required by law, in accordance with § 164.512(a); when needed for oversight of the covered health care provider who created the psychotherapy notes, in accordance with § 164.512(d); when needed by a coroner or medical examiner, in accordance with § 164.512(g)(1); or when needed to avert a serious and imminent threat to health or safety, in accordance with § 164.512(j)(1)(i).

Comment: A commenter suggested that we follow the federal regulations governing confidentiality of alcohol and substance abuse records as a model for limited disclosure of psychotherapy notes for audits or evaluations. Under these regulations, a third party payor or a party providing financial assistance may access confidential records for auditing purposes if the party agrees in writing to keep the records secure and destroy any identifying information upon completion of the audit. (42 CFR part 2)

Response: We agree that the federal regulations concerning alcohol and drug abuse provide a good model for protection of information. However, according to our fact-finding discussions, audit or evaluation should not require access to psychotherapy notes. Protected health information kept in the medical record about an individual should be sufficient for these purposes. The final rule does not require authorization for use or disclosure of psychotherapy notes when needed for oversight of the covered health care provider who created the psychotherapy notes.

Comment: A provider organization urged that the disclosure of psychotherapy notes be strictly prohibited except to the extent needed in litigation brought by the client against the mental health professional on the grounds of professional malpractice or disclosure in violation of this section.

Response: We agree that psychotherapy notes should be available for the defense of the provider who created the notes when the individual who is the subject of the notes puts the contents of the notes at issue in a legal case. In the final rule, we allow the provider to disclose the notes to his or her lawyer for the purpose of preparing a defense. Any other disclosure related to judicial and administrative proceedings is governed by § 164.512(e).

Comment: One commenter requested that we prohibit mental health information that has been disclosed from being re-disclosed without patient authorization.

Response: Psychotherapy notes may only be disclosed pursuant to an authorization, except under limited circumstances. Covered entities must adhere to the terms of authorization and not disclose psychotherapy notes to persons other than those identified as intended recipients or for other purposes. A covered entity that receives psychotherapy notes must adhere to the terms of this rule—including obtaining an authorization for any further use or disclosure. We do not have the authority, however, to prohibit non-covered entities from re-disclosing psychotherapy notes or any other protected health information.

Comment: A provider organization argued for inclusion of language in the final rule that specifies that real or perceived ''ownership'' of the mental health record does not negate the requirement that patients must specifically authorize the disclosure of their psychotherapy notes. They cited a July 1999 National Mental Health Association survey, which found that for purposes of utilization review, every managed care plan policy reviewed ''maintains the right to access the full medical record (including detailed psychotherapy notes) of any consumer covered under its benefit plan at its whim.'' At least one of the major managed health plans surveyed considered the patient record to be the property of the health plan and governed by the health plan's policies.

Response: Although a covered entity may own a mental health record, the ability to use or disclose an individual's information is limited by state law and this rule. Under this rule, a mental health plan would not have access to psychotherapy notes created by a covered provider unless the individual who is the subject of the notes authorized disclosure to the health plan.

Comment: Some commenters expressed concern regarding the burden created by having to obtain multiple authorizations and requested clarification as to whether separate authorization for use and disclosure of psychotherapy notes is required.

Response: For the reasons explained above, we retain in the final rule a requirement that a separate authorization must be obtained for most uses or disclosures of psychotherapy notes, including those for treatment, payment, and health care operations. The burden of such a requirement is extremely low, however, because under our definition of psychotherapy notes, the need for such authorization will be very rare.

Comment: One commenter stated that Medicare should not be able to require the disclosure of psychotherapy notes because it would destroy a practitioner's ability to treat patients effectively.

Response: We agree. As in the proposed rule, covered entities may not disclose psychotherapy notes for payment purposes without an authorization. If a specific provision of law requires the disclosure of these notes, a covered entity may make the disclosure under § 164.512(a). The final rule, however, does not require the disclosure of these notes to Medicare.

Comment: One commenter expressed concern that by filing a complaint an

individual would be required to reveal sensitive information to the public. Another commenter suggested that complaints regarding noncompliance in regard to psychotherapy notes should be made to a panel of mental health professionals designated by the Secretary. This commenter also proposed that all patient information would be maintained as privileged, would not be revealed to the public, and would be kept under seal after the case is reviewed and closed.

Response: We appreciate this concern and the Secretary will ensure that individually identifiable health information and other personal information contained in complaints will not be available to the public. This Department seeks to protect the privacy of individuals to the fullest extent possible, while permitting the exchange of records required to fulfill its administrative and program responsibilities. The Freedom of Information Act, 5 U.S.C. 552, and the HHS implementing regulation, 45 CFR part 5, protect records about individuals if the disclosure would constitute an unwarranted invasion of their personal privacy, as does the Privacy Act, 5 U.S.C. 552a. See the discussion of FOIA and the Privacy Act in the ''Relationship to Other Federal Laws'' section of the preamble. Information that the Secretary routinely withholds from the public in its current enforcement activities includes individual names, addresses, and medical information. Additionally, the Secretary attempts to guard against the release of information that might involve a violation of personal privacy by someone being able to ''read between the lines'' and piece together items that would constitute information that normally would be protected from release to the public. In implementing the privacy rule, the Secretary will continue this practice of protecting personal information.

It is not clear whether the commenter with regard to the use of mental health professionals believes that such professionals should be involved because they would be best able to keep psychotherapy notes confidential or because such professionals can best understand the meaning or relevance of such notes. We anticipate that we would not have to obtain a copy or review psychotherapy notes in investigating most complaints regarding noncompliance in regard to such notes. There may be some cases in which a quick review of the notes may be needed, such as when we need to identify that the information a covered entity disclosed was in fact psychotherapy notes. If we need to obtain a copy of psychotherapy notes, we will keep these notes confidential and secure. Investigative staff will be trained in privacy to ensure that they fully respect the confidentiality of personal information. In addition, while the content of these notes is generally not relevant to violations under this rule, we will secure the expertise of mental health professionals if needed in reviewing psychotherapy notes.

Comment: A mental health organization recommended prohibiting health plans and covered health care providers from disclosing psychotherapy notes to coroners or medical examiners.

Response: In general, we have severely limited disclosures of psychotherapy notes without the individual's authorization. One case where the information may prove invaluable, but authorization by the individual is impossible and authorization by a surrogate is potentially contraindicated, is in the investigation of the death of the individual. The final rule allows for disclosures to coroners or medical examiners in this limited case.

Comment: One commenter recommended prohibiting disclosure without authorization of psychotherapy notes to government health data systems.

Response: The decision to eliminate the general provision permitting disclosures to government health data systems addresses this comment.

Comment: Several commenters were concerned that in practice, a treatment team in a mental health facility shares information about a patient in order to care for the patient and that the provision requiring authorization for use and disclosure of psychotherapy notes would expose almost all privileged information to disclosure. They requested that we add a provision that any authorization or disclosure under that statute shall not constitute a waiver of the psychotherapist-patient privilege.

Response: Because of the restricted definition we have adopted for psychotherapy notes, we do not expect that members of a team will share such information. Information shared in order to care for the patient is, by definition, not protected as psychotherapy notes. With respect to waiving privilege, however, we believe that the consents and authorizations described in §§ 164.506 and 164.508 should not be construed as waivers of a patient's evidentiary privilege. See the discussions under § 164.506 and ''Relationship to Other Laws,'' above.

Research Information Unrelated to Treatment

Definition of Research Information Unrelated to Treatment

Comment: The majority of commenters, including many researchers and health care providers, objected to the proposed definition of research information unrelated to treatment, asserting that the privacy rule should not distinguish research information unrelated to treatment from other forms of protected health information. Even those who supported the proposed distinction between research information related and unrelated to treatment suggested alternative definitions for research information unrelated to treatment.

A large number of commenters were concerned that the definition of research information unrelated to treatment was vague and unclear and, therefore, would be difficult or impossible to apply. These commenters asserted that in many instances it would not be feasible to ascertain whether research information bore some relation to treatment. In addition, several commenters asserted that the need for distinguishing research information unrelated to treatment from other forms of protected health information was not necessary because the proposed rule's general restrictions for the use and disclosure of protected health information and the existing protections for research information were sufficiently strong.

Of the commenters who supported the proposed distinction between research information related and unrelated to treatment, very few supported the proposed definition of research unrelated to treatment. A few commenters recommended that the definition incorporate a good faith provision and apply only to health care providers, because they thought it was unlikely that a health plan or health care clearinghouse would be conducting research. One commenter recommended defining research information unrelated to treatment as information which does not directly affect the treatment of the individual patient. As a means of clarifying and standardizing the application of this definition, one commenter also asserted that the definition should be based on whether the research information was for publication. In addition, one commenter specifically objected to the provision of the proposed definition that would have required that research information unrelated to treatment be information ''with respect to which the covered entity has not requested payment from

a third party payor.'' This commenter asserted that patient protection should not be dependent on whether a health plan will pay for certain care.

Response: We agree with the commenters who found the proposed definition of research information unrelated to treatment to be impractical and infeasible to apply and have eliminated this definition and its related provisions in the final rule. Although we share concerns raised by some commenters that research information generated from research studies that involve the delivery of treatment to individual subjects may need additional privacy protection, we agree with the commenters who asserted that there is not always a clear distinction between research information that is related to treatment and research information that is not. We found that the alternative definitions proposed by commenters did not alleviate the serious concerns raised by the majority of comments received on this definition.

Instead, in the final rule, we require covered entities that create protected health information for the purpose, in whole or in part, of research that includes treatment of individuals to include additional elements in authorizations they request for the use or disclosure of that protected health information. As discussed in § 164.508(f), these research-related authorizations must include a description of the extent to which some or all of the protected health information created for the research will also be used or disclosed for purposes of treatment, payment, and health care operations. For example, if the covered entity intends to seek reimbursement from the individual's health plan for the routine costs of care associated with the research protocol, it must explain in the authorization the types of information that it will provide to the health plan for this purpose. This information, and the circumstances under which disclosures will be made for treatment, payment, and health care operations, may be more limited than the information and circumstances described in the covered entity's general notice of information practices and are binding on the covered entity.

Under this approach, the covered entity that creates protected health information for research has discretion to determine whether there is a subset of research information that will have fewer allowable disclosures without authorization, and prospective research subjects will be informed about how research information about them would be used and disclosed should they agree to participate in the research study. We believe this provision in the final rule provides covered entities that participate in research necessary flexibility to enhance privacy protections for research information and provides prospective research subjects with needed information to determine whether their privacy interests would be adequately protected before agreeing to participate in a research study that involves the delivery of health care.

The intent of this provision is to permit covered entities that participate in research to bind themselves to a more limited scope of uses and disclosures for all or identified subsets of research information generated from research that involves the delivery of treatment than it may apply to other protected health information. In designing their authorizations, we expect covered entities to be mindful of the often highly sensitive nature of research information and the impact of individuals' privacy concerns on their willingness to participate in research. For example, a covered entity conducting a study which involves the evaluation of a new drug, as well as an assessment of a new un-validated genetic marker of a particular disease, could choose to stipulate in the research authorization that the genetic information generated from this study will not be disclosed without authorization for some of the public policy purposes that would otherwise be permitted by the rule under §§ 164.510 and 164.512 and by the covered entity's notice. A covered entity may not, however, include a limitation affecting its right to make a use or disclosure that is either required by law or is necessary to avert a serious and imminent threat to health or safety.

The final rule also permits the covered entity to combine the research authorization under § 164.508(f) with the consent to participate in research, such as the informed consent document as stipulated under the Common Rule or the Food and Drug Administration's human subjects regulations.

Enhance Privacy Protections for Research Information

Comment: A number of commenters argued that research information unrelated to treatment should have fewer allowable disclosures without authorization than those that would have been permitted by the proposed rule. The commenters who made this argument included those commenters who recommended that the privacy rule not cover the information we proposed to constitute research information unrelated to treatment, as well as those who asserted that the rule should cover such information. These commenters agreed with the concern expressed in the proposed rule that patients would be reluctant to participate in research if they feared that research information could be disclosed without their permission or used against them. They argued that fewer allowable disclosures should be permitted for research information because the clinical utility of the research information is most often unknown, and thus, it is unsuitable for use in clinical decision making. Others also argued that it is critical to the conduct of clinical research that researchers be able to provide individual research subjects, and the public at large, the greatest possible assurance that their privacy and the confidentiality of any individually identifiable research information will be protected from disclosure.

Several commenters further recommended that only the following uses and disclosures be permitted for research information unrelated to treatment without authorization: (1) For the oversight of the researcher or the research study; (2) for safety and efficacy reporting required by FDA; (3) for public health; (4) for emergency circumstances; or (5) for another research study. Other commenters recommended that the final rule explicitly prohibit law enforcement officials from gaining access to research records.

In addition, several commenters asserted that the rule should be revised to ensure that once protected health information was classified as research information unrelated to treatment, it could not be re-classified as something else at a later date. These commenters believed that if this additional protection were not added, this information would be vulnerable to disclosure in the future, if the information were later to gain scientific validity. They argued that individuals may rely on this higher degree of confidentiality when consenting to the collection of the information in the first instance, and that confidentiality should not be betrayed in the future just because the utility of the information has changed.

Response: We agree with commenters who argued that special protections may be appropriate for research information in order to provide research subjects with assurances that their decision to participate in research will not result in harm stemming from the misuse of the research information. We are aware that some researchers currently retain separate research records and medical records as a means of providing more stringent privacy protections for the research record. The final rule permits

covered entities that participate in research to continue to provide more stringent privacy protections for the research record, and the Secretary strongly encourages this practice to protect research participants from being harmed by the misuse of their research information.

As discussed above, in the final rule, we eliminate the special rules for this proposed definition of research information unrelated to treatment and its related provisions, so the comments regarding its application are moot.

Comment: Some commenters recommended that the final rule prohibit a covered entity from conditioning treatment, enrollment in a health plan, or payment on a requirement that the individual authorize the use or disclosure of information we proposed to constitute research information unrelated to treatment.

Response: Our decision to eliminate the definition of research information unrelated to treatment and its related provisions in the final rule renders this comment moot.

Comment: A few commenters opposed distinguishing between research information related to treatment and research information unrelated to treatment, arguing that such a distinction could actually weaken the protection afforded to clinically-related health information that is collected in clinical trials. These commenters asserted that Certificates of Confidentiality shield researchers from being compelled to disclose individually identifiable health information relating to biomedical or behavioral research information that an investigator considers sensitive.

Response: Our decision to eliminate the definition of research information unrelated to treatment and its related provisions in the final rule renders this comment moot. We would note that nothing in the final rule overrides Certificates of Confidentiality, which protect against the compelled disclosure of identifying information about subjects of biomedical, behavioral, clinical, and other research as provided by the Public Health Service Act section 301(d), 42 U.S.C. 241(d).

Privacy Protections for Research Information Too Stringent

Comment: Many of the commenters who opposed the proposed definition of research information unrelated to treatment and its related provisions believed that the proposed rule would have required authorization before research information unrelated to treatment could have been used or disclosed for any of the public policy purposes outlined in proposed § 164.510, and that this restriction would have significantly hindered many important activities. Many of these commenters specifically opposed this provision, arguing that the distinction would undermine and impede research by requiring patient authorization before research information unrelated to treatment could be used or disclosed for research.

Furthermore, some commenters recommended that the disclosure of research information should be governed by an informed consent agreement already in place as part of a clinical protocol, or its disclosure should be considered by an institutional review board or privacy board.

Response: Our decision to eliminate the definition of research information unrelated to treatment and its related provisions in the final rule renders the first two comments moot.

We disagree with the comment that suggests that existing provisions under the Common Rule are sufficient to protect the privacy interests of individuals who are subjects in research that involves the delivery of treatment. As discussed in the NPRM, not all research is subject to the Common Rule. In addition, we are not convinced that existing procedures adequately inform individuals about how their information will be used as part of the informed consent process. In the final rule, we provide for additional disclosure to subjects of research that involves the delivery of treatment as part of the research authorization under § 164.508(f). We also clarify that the research authorization could be combined with the consent to participate in research, such as the informed consent document as stipulated under the Common Rule or the Food and Drug Administration's human subjects regulations. The Common Rule (§_.116(a)(5)) requires that ''informed consent'' include ''a statement describing the extent, if any, to which confidentiality of records identifying the subject will be maintained.'' We believe that the research authorization requirements of § 164.508(f) complement the Common Rule's requirement for informed consent.

The Secretary's Authority

Comment: Several commenters, many from the research community, asserted that the coverage of ''research information unrelated to treatment'' was beyond the Department's legal authority since HIPAA did not give the Secretary authority to regulate researchers. These commenters argued that the research records held by researchers who are performing clinical trials and who keep separate research records should not be subject to the final rule. These commenters strongly disagreed that a health provider-researcher cannot carry out two distinct functions while performing research and providing clinical care to research subjects and, thus, asserted that research information unrelated to treatment that is kept separate from the medical record, would not be covered by the privacy rule.

Response: We do not agree the Secretary lacks the authority to adopt standards relating to research information, including research information unrelated to treatment. HIPAA provides authority for the Secretary to set standards for the use and disclosure of individually identifiable health information created or received by covered entities. For the reasons commenters identified for why it was not practical or feasible to divide research information into two categories—research information related to treatment and research information unrelated to treatment—we also determined that for a single research study that includes the treatment of research subjects, it is not practical or feasible to divide a researcher into two categories—a researcher who provides treatment and a researcher who does not provide treatment to research subjects. When a researcher is interacting with research subjects for a research study that involves the delivery of health care to subjects, it is not always clear to either the researcher or the research subject whether a particular research activity will generate research information that will be pertinent to the health care of the research subject. Therefore, we clarify that a researcher may also be a health care provider if that researcher provides health care, *e.g.,* provides treatment to subjects in a research study, and otherwise meets the definition of a health care provider, regardless of whether there is a component of the research study that is unrelated to the health care of the research subjects. This researcher/health care provider is then a covered entity with regard to her provider activities if she conducts standard transactions.

Valid Authorizations

Comment: In proposed § 164.508(b)(1), we specified that an authorization containing the applicable required elements ''must be accepted by the covered entity.'' A few comments requested clarification of this requirement.

Response: We agree with the commenters that the proposed provision was ambiguous and we remove it from the final rule. We note that nothing in the rule requires covered entities to act on authorizations that they receive, even if those authorizations are valid. A covered entity presented with an authorization is permitted to make the disclosure authorized, but is not required to do so.

We want to be clear, however, that covered entities will be in compliance with this rule if they use or disclose protected health information pursuant to an authorization that meets the requirements of § 164.508. We have made changes in § 164.508(b)(1) to clarify this point. First, we specify that an authorization containing the applicable required elements is a valid authorization. A covered entity may not reject as invalid an authorization containing such elements. Second, we clarify that a valid authorization may contain elements or information in addition to the required elements, as long as the additional elements are not inconsistent with the required elements.

Comment: A few comments requested that we provide a model authorization or examples of wording meeting the ''plain language'' requirement. One commenter requested changes to the language in the model authorization to avoid confusion when used in conjunction with an insurer's authorization form for application for life or disability income insurance. Many other comments, however, found fault with the proposed model authorization form.

Response: Because of the myriad of types of forms that could meet these requirements and the desire to encourage covered entities to develop forms that meet their specific needs, we do not include a model authorization form in the final rule. We intend to issue additional guidance about authorization forms prior to the compliance date. We also encourage standard-setting organizations to develop model forms meeting the requirements of this rule.

Defective Authorizations

Comment: Some commenters suggested we insert a ''good-faith reliance'' or ''substantial compliance'' standard into the authorization requirements. Commenters suggested that covered entities should be permitted to rely on an authorization as long as the individual has signed and dated the document. They stated that individuals may not fill out portions of a form that they feel are irrelevant or for which they do not have an answer. They argued that requiring covered entities to follow up with each individual to complete the form will cause unwarranted delays. In addition, commenters were concerned that large covered entities might act in good faith on a completed authorization, only to find out that a component of the entity ''knew'' some of the information on the form to be false or that the authorization had been revoked. These commenters did not feel that covered entities should be held in violation of the rule in such situations.

Response: We retain the provision as proposed and include one additional element: the authorization is invalid if it is combined with other documents in violation of the standards for compound authorizations. We also clarify that an authorization is invalid if material information on the form is known to be false. The elements we require to be included in the authorization are intended to ensure that individuals knowingly and willingly authorize the use or disclosure of protected health information about them. If these elements are missing or incomplete, the covered entity cannot know which protected health information to use or disclose to whom and cannot be confident that the individual intends for the use or disclosure to occur.

We have attempted to make the standards for defective authorizations as unambiguous as possible. In most cases, the covered entity will know whether the authorization is defective by looking at the form itself. Otherwise, the covered entity must know that the authorization has been revoked, that material information on the form is false, or that the expiration date or event has occurred. If the covered entity does not know these things and the authorization is otherwise satisfactory on its face, the covered entity is permitted to make the use or disclosure in compliance with this rule.

We have added two provisions to make it easier for covered entities to ''know'' when an authorization has been revoked. First, under § 164.508(b)(5), the revocation must be made in writing. Second, under § 164.508(c)(1)(v), authorizations must include instructions for how the individual may revoke the authorization. Written revocations submitted in the manner appropriate for the covered entity should ease covered entities' compliance burden.

Compound Authorizations

Comment: Many commenters raised concerns about the specificity of the authorization requirement. Some comments recommended that we permit covered entities to include multiple uses and disclosures in a single authorization and allow individuals to authorize or not authorize specific uses and disclosures in the authorization. Other commenters asked whether a single authorization is sufficient for multiple uses or disclosures for the same purpose, for multiple uses and disclosures for related purposes, and for uses and disclosures of different types of information for the same purpose. Some comments from health care providers noted that specific authorizations would aid their compliance with requests.

Response: As a general rule, we prohibit covered entities from combining an authorization for the use or disclosure of protected health information with any other document. For example, an authorization may not be combined with a consent to receive treatment or a consent to assign payment of benefits to a provider. We intend the authorizations required under this rule to be voluntary for individuals, and, therefore, they need to be separate from other forms of consent that may be a condition of treatment or payment or that may otherwise be coerced.

We do, however, permit covered entities to combine authorizations for uses and disclosures for multiple purposes into a single authorization. The only limitations are that an authorization for the use or disclosure of psychotherapy notes may not be combined with an authorization for the use or disclosure of other types of protected health information and that an authorization that is a condition of treatment, payment, enrollment, or eligibility may not be combined with any other authorization.

In § 164.508(b)(3), we also permit covered entities to combine an authorization for the use or disclosure of protected health information created for purposes of research including treatment of individuals with certain other documents.

We note that covered entities may only make uses or disclosures pursuant to an authorization that are consistent with the terms of the authorization. Therefore, if an individual agrees to one of the disclosures described in the compound authorization but not another, the covered entity must comply with the individual's decision. For example, if a covered entity asks an individual to sign an authorization to disclose protected health information for both marketing and fundraising purposes, but the individual only agrees to the fundraising disclosure, the

covered entity is not permitted to make the marketing disclosure.

Prohibition on Conditioning Treatment, Payment, Eligibility, or Enrollment

Comment: Many commenters supported the NPRM's prohibition of covered entities from conditioning treatment or payment on the individual's authorization of uses and disclosures. Some commenters requested clarification that employment can be conditioned on an authorization. Some commenters recommended that we eliminate the requirement for covered entities to state on the authorization form that the authorization is not a condition of treatment or payment. Some commenters suggested that we prohibit the provision of anything of value, including employment, from being conditioned on receipt of an authorization.

In addition, many commenters argued that patients should not be coerced into signing authorizations for a wide variety of purposes as a condition of obtaining insurance coverage. Some health plans, however, requested clarification that health plan enrollment and eligibility can be conditioned on an authorization.

Response: We proposed to prohibit covered entities from conditioning treatment, payment, or enrollment in a health plan on an authorization for the use or disclosure of psychotherapy notes (see proposed § 164.508(a)(3)(iii)). We proposed to prohibit covered entities from conditioning treatment or payment on authorization for the use or disclosure of any other protected health information (see proposed § 164.508(a)(2)(iii)).

We resolve this inconsistency by clarifying in § 164.508(b)(4) that, with certain exceptions, a covered entity may not condition the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits on an authorization for the use or disclosure of any protected health information, including psychotherapy notes. We intend to minimize the potential for covered entities to coerce individuals into signing authorizations for the use or disclosure of protected health information when such information is not essential to carrying out the relationship between the individual and the covered entity.

Pursuant to that goal, we have created limited exceptions to the prohibition. First, a covered health care provider may condition research-related treatment of an individual on obtaining the individual's authorization to use or disclose protected health information created for the research. Second, except with respect to psychotherapy notes, a health plan may condition the individual's enrollment or eligibility in the health plan on obtaining an authorization for the use or disclosure of protected health information for making enrollment or eligibility determinations relating to the individual or for its underwriting or risk rating determinations. Third, a health plan may condition payment of a claim for specified benefits on obtaining an authorization under § 164.508(e) for disclosure to the plan of protected health information necessary to determine payment of the claim. Fourth, a covered entity may condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party (such as fitness-for-duty exams and physicals necessary to obtain life insurance coverage) on obtaining an authorization for the disclosure of the protected health information. We recognize that covered entities need protected health information in order to carry out these functions and provide services to the individual; therefore, we allow authorization for the disclosure of the protected health information to be a condition of obtaining the services.

We believe that we have prohibited covered entities from conditioning the services they provide to individuals on obtaining an authorization for uses and disclosures that are not essential to those services. Due to our limited authority, however, we cannot entirely prevent individuals from being coerced into signing these forms. We do not, for example, have the authority to prohibit an employer from requiring its employees to sign an authorization as a condition of employment. Similarly, a program such as the Job Corps may make such an authorization a condition of enrollment in the Job Corps program. While the Job Corps may include a health care component, the non-covered component of the Job Corps may require as a condition of enrollment that the individual authorize the health care component to disclose protected health information to the non-covered component. See § 164.504(b). However, we note that other nondiscrimination laws may limit the ability to condition these authorizations as well.

Comment: A Medicaid fraud control association stated that many states require or permit state Medicaid agencies to obtain an authorization for the use and disclosure of protected health information for payment purposes as a condition of enrolling an individual as a Medicaid recipient. The commenter, therefore, urged an exception to the prohibition on conditioning enrollment on obtaining an authorization.

Response: As explained above, under § 164.506(a)(4), health plans and other covered entities may seek the individual's consent for the covered entity's use and disclosure of protected health information to carry out treatment, payment, or health care operations. If the consent is sought in conjunction with enrollment, the health plan may condition enrollment in the plan on obtaining the individual's consent.

Under § 164.506(a)(5), we specify that a consent obtained by one covered entity is not effective to permit another covered entity to use or disclose protected health information for payment purposes. If state law requires a Medicaid agency to obtain the individual's authorization for providers to disclose protected health information to the Medicaid agency for payment purposes, the agency may do so under § 164.508(e). This authorization must not be a condition of enrollment or eligibility, but may be a condition of payment of a claim for specified benefits if the disclosure is necessary to determine payment of the claim.

Revocation of Authorizations

Comment: Many commenters supported the right to revoke an authorization. Some comments, however, suggested that we require authorizations to remain valid for a minimum period of time, such as one year or the duration of the individual's enrollment in a health plan.

Response: We retain the right for individuals to revoke an authorization at any time, with certain exceptions. We believe this right is essential to ensuring that the authorization is voluntary. If an individual determines that an authorized use or disclosure is no longer in her best interest, she should be able to withdraw the authorization and prevent any further uses or disclosures.

Comment: Several commenters suggested that we not permit individuals to revoke an authorization if the revocation would prevent an investigation of material misrepresentation or fraud. Other commenters similarly suggested that we not permit individuals to revoke an authorization prior to a claim for benefits if the insurance was issued in reliance on the authorization.

Response: To address this concern, we include an additional exception to the right to revoke an authorization. Individuals do not have the right to revoke an authorization that was obtained as a condition of insurance coverage during any contestability

period under other law. For example, if a life insurer obtains the individual's authorization for the use or disclosure of protected health information to determine eligibility or premiums under the policy, the individual does not have the right to revoke the authorization during any period of time in which the life insurer can contest a claim for benefits under the policy in accordance with state law. If an individual were able to revoke the authorization after enrollment but prior to making a claim, the insurer would be forced to pay claims without having the necessary information to determine whether the benefit is due. We believe the existing exception for covered entities that have acted in reliance on the authorization is insufficient to address this concern because it is another person, not the covered entity, that has acted in reliance on the authorization. In the life insurance example, it is the life insurer that has taken action (i.e., issued the policy) in reliance on the authorization. The life insurer is not a covered entity, therefore the covered entity exception is inapplicable.

Comment: Some comments suggested that a covered entity that had compiled, but not yet disclosed, protected health information would have already taken action in reliance on the authorization and could therefore disclose the information even if the individual revoked the authorization.

Response: We intend for covered entities to refrain from further using or disclosing protected health information to the maximum extent possible once an authorization is revoked. The exception exists only to the extent the covered entity has taken action in reliance on the authorization. If the covered entity has not yet used or disclosed the protected health information, it must refrain from doing so, pursuant to the revocation. If, however, the covered entity has already disclosed the information, it is not required to retrieve the information.

Comment: One comment suggested that the rule allow protected health information to be only rented, not sold, because there can be no right to revoke authorization for disclosure of protected health information that has been sold.

Response: We believe this limitation would be an unwarranted abrogation of covered entities' business practices and outside the scope of our authority. We believe individuals should have the right to authorize any uses or disclosures they feel are appropriate. We have attempted to create authorization requirements that make the individual's decisions as clear and voluntary as possible.

Comment: One commenter expressed concern as to whether the proposed rule's standard to protect the protected health information about a deceased individual for two years would interfere with the payment of death benefit claims. The commenter asked that the regulation permit the beneficiary or payee under a life insurance policy to authorize disclosure of protected health information pertaining to the cause of death of a decedent or policyholder. Specifically, the commenter explained that when substantiating a claim a beneficiary, such as a fiancee or friend, may be unable to obtain the authorization required to release information to the insurer, particularly if, for example, the decedent's estate does not require probate or if the beneficiary is not on good terms with the decedent's next of kin. Further, the commenter stated that particularly in cases where the policyholder dies within two years of the policy's issuance (within the policy's contestable period) and the cause of death is uncertain, the insurer's inability to access relevant protected health information would significantly interfere with claim payments and increase administrative costs.

Response: We do not believe this will be a problem under the final regulation, because we create an exception to the right to revoke an authorization if the authorization was obtained as a condition of obtaining insurance coverage and other applicable law provides the insurer that obtained the authorization with the right to contest a claim under the policy. Thus, if a policyholder dies within the two year contestability period, the authorization the insurer obtained from the policyholder prior to death could not be revoked during the contestability period.

Core Elements and Requirements

Comment: Many commenters raised concerns about the required elements for a valid authorization. They argued that the requirements were overly burdensome and that covered entities should have greater flexibility to craft authorizations that meet their business needs. Other commenters supported the required elements as proposed because the elements help to ensure that individuals make meaningful, informed choices about the use and disclosure of protected health information about them.

Response: As in the proposed rule, we define specific elements that must be included in any authorization. We draw on established laws and guidelines for these requirements. For example, the July 1977 Report of the Privacy Protection Study Commission recommended that authorizations obtained by insurance institutions include plain language, the date of authorization, and identification of the entities authorized to disclose information, the nature of the information to be disclosed, the entities authorized to receive information, the purpose(s) for which the information may be used by the recipients, and an expiration date.[13] The Commission made similar recommendations concerning the content of authorizations obtained by health care providers.[14] The National Association of Insurance Commissioners' Health Information Privacy Model Act requires authorizations to be in writing and include a description of the types of protected health information to be used or disclosed, the name and address of the person to whom the information is to be disclosed, the purpose of the authorization, the signature of the individual or the individual's representative, and a statement that the individual may revoke the authorization at any time, subject to the rights of any person that acted in reliance on the authorization prior to revocation and provided the revocation is in writing, dated, and signed. Standards of the American Society for Testing and Materials recommend that authorizations identify the subject of the protected health information to be disclosed; the name of the person or institution that is to release the information; the name of each individual or institution that is to receive the information; the purpose or need for the information; the information to be disclosed; the specific date, event, or condition upon which the authorization will expire, unless revoked earlier; and the signature and date signed. They also recommend the authorization include a statement that the authorization can be revoked or amended, but not retroactive to a release made in reliance on the authorization.[15]

Comment: Some commenters requested clarification that authorizations ''initiated by the individual'' include authorizations initiated by the individual's representative.

---

[13] Privacy Protection Study Commission, ''Personal Privacy in an Information Society,'' July 1977, p. 196–197.

[14] Privacy Protection Study Commission, ''Personal Privacy in an Information Society,'' July 1977, p. 315.

[15] ASTM, ''Standard Guide for Confidentiality, Privacy, Access and Data Security, Principles for Health Information Including Computer-Based Patient Records,'' E 1869–97, § 12.1.4.

Response: In the final rule, we do not classify authorizations as those initiated by the individual versus those initiated by a covered entity. Instead, we establish a core set of elements and requirements that apply to all authorizations and require certain additional elements for particular types of authorizations initiated by covered entities.

Comment: Some commenters urged us to permit authorizations that designate a class of entities, rather than specifically named entities, that are authorized to use or disclose protected health information. Commenters made similar recommendations with respect to the authorized recipients. Commenters suggested these changes to prevent covered entities from having to seek, and individuals from having to sign, multiple authorizations for the same purpose.

Response: We agree. Under § 164.508(c)(1), we require authorizations to identify both the person(s) authorized to use or disclose the protected health information and the person(s) authorized to receive protected health information. In both cases, we permit the authorization to identify either a specific person or a class of persons.

Comment: Many commenters requested clarification that covered entities may rely on electronic authorizations, including electronic signatures.

Response: All authorizations must be in writing and signed. We intend e-mail and electronic documents to qualify as written documents. Electronic signatures are sufficient, provided they meet standards to be adopted under HIPAA. In addition, we do not intend to interfere with the application of the Electronic Signature in Global and National Commerce Act.

Comment: Some commenters requested that we permit covered entities to use and disclose protected health information pursuant to verbal authorizations.

Response: To ensure compliance and mutual understanding between covered entities and individuals, we require all authorizations to be in writing.

Comment: Some commenters asked whether covered entities can rely on copies of authorizations rather than the original. Other comments asked whether covered entities can rely on the assurances of a third party, such as a government entity, that a valid authorization has been obtained to use or disclose protected health information. These commenters suggested that such procedures would promote the timely provision of benefits for programs that require the collection of protected health information from multiple sources, such as determinations of eligibility for disability benefits.

Response: Covered entities must obtain the individual's authorization to use or disclose protected health information for any purpose not otherwise permitted or required under this rule. They may obtain this authorization directly from the individual or from a third party, such as a government agency, on the individual's behalf. In accordance with the requirements of § 164.530(j), the covered entity must retain a written record of authorization forms signed by the individual. Covered entities must, therefore, obtain the authorization in writing. They may not rely on assurances from others that a proper authorization exists. They may, however, rely on copies of authorizations if doing so is consistent with other law.

Comment: We requested comments on reasonable steps that a covered entity could take to be assured that the individual who requests the disclosure is whom she or he purports to be. Some commenters stated that it would be extremely difficult to verify the identity of the person signing the authorization, particularly when the authorization is not obtained in person. Other comments recommended requiring authorizations to be notarized.

Response: To reduce burden on covered entities, we are not requiring verification of the identities of individuals signing authorization forms or notarization of the forms.

Comment: A few commenters asked for clarification regarding the circumstances in which a covered entity may consider a non-response as an authorization.

Response: Non-responses to requests for authorizations cannot be considered authorizations. Authorizations must be signed and have the other elements of a valid authorization described above.

Comment: Most commenters generally supported the requirement for an expiration date on the authorization. Commenters recommended expiration dates from 6 months to 3 years and/or proposed that the expiration be tied to an event such as duration of enrollment or when an individual changes health plans. Others requested no expiration requirement for some or all authorizations.

Response: We have clarified that an authorization may include an expiration date in the form of a specific date, a specific time period, or an event directly related to the individual or the purpose of the authorization. For example, a valid authorization could expire upon the individual's disenrollment from a health plan or upon termination of a research project. We prohibit an authorization from having an indeterminate expiration date.

These changes were intended to address situations in which a specific date for the termination of the purpose for the authorization is difficult to determine. An example may be a research study where it may be difficult to predetermine the length of the project.

Comment: A few commenters requested that the named insured be permitted to sign an authorization on behalf of dependents.

Response: We disagree with the commenter that a named insured should always be able to authorize uses and disclosures for other individuals in the family. Many dependents under group health plans have their own rights under this rule, and we do not assume that one member of a family has the authority to authorize uses or disclosures of the protected health information of other family members.

A named insured may sign a valid authorization for an individual if the named insured is a personal representative for the individual in accordance with § 164.502(g). The determination of whether an individual is a personal representative under this rule is based on other applicable law that determines when a person can act on behalf of an individual in making decisions related to health care. This rule limits a person's rights and authorities as a personal representative to only the protected health information relevant to the matter for which he or she is a personal representative under other law. For example, a parent may be a personal representative of a child for most health care treatment and payment decisions under state law. In that case, a parent, who is a named insured for her minor child, would be able to provide authorization with respect to most protected health information about her dependent child. However, a wife who is the named insured for her husband who is a dependent under a health insurance policy may not be a personal representative for her husband under other law or may be a personal representative only for limited purposes, such as for making decisions regarding payment of disputed claims. In this case, she may have limited authority to access protected health information related to the payment of disputed claims, but would not have the authority to authorize that her husband's information be used for

marketing purposes, absent any other authority to act for her husband. See § 164.502(g) for more information regarding personal representatives.

Comment: One commenter suggested that authorizations should be dated on the day they are signed.

Response: We agree and have retained this requirement in the final rule.

Additional Elements and Requirements for Authorizations Requested by the Covered Entity for Its Own Uses and Disclosures

Comment: Some commenters suggested that we should not require different elements in authorizations initiated by the covered entity versus authorizations initiated by the individual. The commenters argued the standards were unnecessary, confusing, and burdensome.

Response: The proposed authorization requirements are intended to ensure that an individual's authorization is truly voluntary. The additional elements required for authorizations initiated by the covered entity for its own uses and disclosures or for receipt of protected health information from other covered entities to carry out treatment, payment, or health care operations address concerns that are unique to these forms of authorization. (See above regarding requirements for research authorizations under § 164.508(f).)

First, when applicable, these authorizations must state that the covered entity will not condition treatment, payment, eligibility, or enrollment on the individual's providing authorization for the requested use or disclosure. This statement is not appropriate for authorizations initiated by the individual or another person who does not have the ability to withhold services if the individual does not authorize the use or disclosure.

Second, the authorization must state that the individual may refuse to sign the authorization. This statement is intended to signal to the individual that the authorization is voluntary and may not be accurate if the authorization is obtained by a person other than a covered entity.

Third, these authorizations must describe the purpose of the use or disclosure. We do not include this element in the core requirements because we understand there may be times when the individual does not want the covered entity maintaining the protected health information to know the purpose for the use or disclosure. For example, an individual contemplating litigation may not want the covered entity to know that litigation is the purpose of the disclosure. If the covered entity is initiating the authorization for its own use or disclosure, however, the individual and the covered entity maintaining the protected health information should have a mutual understanding of the purpose of the use or disclosure. Similarly, when a covered entity is requesting authorization for a disclosure by another covered entity that may have already obtained the individual's consent for the disclosure, the individual and covered entity that maintains the protected health information should be aware of this potential conflict.

There are two additional requirements for authorizations requested by a covered entity for its own use or disclosure of protected health information it maintains. First, we require the covered entity to describe the individual's right to inspect or copy the protected health information to be used or disclosed. Individuals may want to review the information to be used or disclosed before signing the authorization and should be reminded of their ability to do so. This requirement is not appropriate for authorizations for a covered entity to receive protected health information from another covered entity, however, because the covered entity requesting the authorization is not the covered entity that maintains the protected health information and cannot, therefore, grant or describe the individual's right to access the information.

If applicable, we also require a covered entity that requests an authorization for its own use or disclosure to state that the use or disclosure of the protected health information will result in direct or indirect remuneration to the entity. Individuals should be aware of any conflicts of interest or financial incentives on the part of the covered entity requesting the use or disclosure. These statements are not appropriate, however, in relation to uses and disclosures to carry out treatment, payment, and health care operations. Uses and disclosures for these purposes will often involve remuneration by the nature of the use or disclosure, not due to any conflict of interest on the part of either covered entity.

We note that authorizations requested by a covered entity include authorizations requested by the covered entity's business associate on the covered entity's behalf. Authorizations requested by a business associate on the covered entity's behalf and that authorize the use or disclosure of protected health information by the covered entity or the business associate must meet the requirements in § 164.508(d). Similarly, authorizations requested by a business associate on behalf of a covered entity to accomplish the disclosure of protected health information to that business associate or covered entity as described in § 164.508(e) must meet the requirements of that provision.

We disagree that these elements are unnecessary, confusing, or burdensome. We require them to ensure that the individual has a complete understanding of what he or she is agreeing to permit.

Comment: Many commenters suggested we include in the regulation text a provision stated in the preamble that entities and their business partners must limit their uses and disclosures to the purpose(s) specified by the individual in the authorization.

Response: We agree. In accordance with § 164.508(a)(1), covered entities may only use or disclose protected health information consistent with the authorization. In accordance with § 164.504(e)(2), a business associate may not make any uses or disclosures that the covered entity couldn't make.

Comment: Some comments suggested that authorizations should identify the source and amount of financial gain, if any, resulting from the proposed disclosure. Others suggested that the proposed financial gain requirements were too burdensome and would decrease trust between patients and providers. Commenters recommended that the requirement either should be eliminated or should only require covered entities, when applicable, to state that direct and foreseeable financial gain to the covered entity will result. Others requested clarification of how the requirement for covered entities to disclose financial gain relates to the criminal penalties that accrue for offenses committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm. Some commenters advocated use of the term ''financial compensation'' rather than ''financial gain'' to avoid confusion with in-kind compensation rules. Some comments additionally suggested excluding marketing uses and disclosures from the requirements regarding financial gain.

Response: We agree that clarification is warranted. In § 164.508(d)(1)(iv) of the final rule, we require a covered entity that asks an individual to sign an authorization for the covered entity's use or disclosure of protected health information and that will receive direct

or indirect remuneration from a third party for the use or disclosure, to state that fact in the authorization. Remuneration from a third party includes payments such as a fixed price per disclosure, compensation for the costs of compiling and sending the information to be disclosed, and, with respect to marketing communications, a percentage of any sales generated by the marketing communication. For example, a device manufacturer may offer to pay a fixed price per name and address of individuals with a particular diagnosis, so that the device manufacturer can market its new device to people with the diagnosis. The device manufacturer may also offer the covered entity a percentage of the profits from any sales generated by the marketing materials sent. If a covered entity seeks an authorization to make such a disclosure, the authorization must state that the remuneration will occur. We believe individuals should have the opportunity to weigh the covered entity's potential conflict of interest when deciding to authorize the covered entity's use or disclosure of protected health information. We believe that the term ''remuneration from a third party'' clarifies our intent to describe a direct, tangible exchange, rather than the mere fact that parties intend to profit from their enterprises.

Comment: One commenter suggested we require covered entities to request authorizations in a manner that does not in itself disclose sensitive information.

Response: We agree that covered entities should make reasonable efforts to avoid unintentional disclosures. In § 164.530(c)(2), we require covered entities to have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

Comment: Some commenters requested clarification that covered entities are permitted to seek authorization at the time of enrollment or when individuals otherwise first interact with covered entities. Similarly, commenters requested clarification that covered entities may disclose protected health information created after the date the authorization was signed but prior to the expiration date of the authorization. These commenters were concerned that otherwise multiple authorizations would be required to accomplish a single purpose. Other comments suggested that we prohibit prospective authorizations (i.e., authorizations requested prior to the creation of the protected health information to be disclosed under the authorization) because it is not possible for individuals to make informed decisions about these authorizations.

Response: We confirm that covered entities may act on authorizations signed in advance of the creation of the protected health information to be released. We note, however, that all of the required elements must be completed, including a description of the protected health information to be used or disclosed pursuant to the authorization. This description must identify the information in a specific and meaningful fashion so that the individual can make an informed decision as to whether to sign the authorization.

Comment: Some commenters suggested that the final rule prohibit financial incentives, such as premium discounts, designed to encourage individuals to sign authorizations.

Response: We do not prohibit or require financial incentives for authorizations. We have attempted to ensure that authorizations are entered into voluntary. If a covered entity chooses to offer a financial incentive for the individual to sign the authorization, and the individual chooses to accept it, they are free to do so.

Section 164.510—Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object

Section 164.510(a)—Use and Disclosure for Facility Directories

Comment: Many hospital organizations opposed the NPRM's proposed opt-in approach to disclosure of directory information. These groups noted the preamble's statement that most patients welcomed the convenience of having their name, location, and general condition included in the patient directory. They said that requiring hospitals to obtain authorization before including patient information in the directory would cause harm to many patients' needs in an effort to serve the needs of the small number of patients who may not want their information to be included. Specifically, they argued that the proposed approach ultimately could have the effect of making it difficult or impossible for clergy, family members, and florists to locate patients for legitimate purposes. In making this argument, commenters pointed to problems that occurred after enactment of privacy legislation in the State of Maine in 1999. The legislation, which never was officially implemented, was interpreted by hospitals to prohibit disclosure of patient information to directories without written consent. As a result, when hospitals began complying with the law based on their interpretation, family members and clergy had difficulty locating patients in the hospital.

Response: We share commenters' concern about the need to ensure that family members and clergy who have a legitimate need to locate patients are not prevented from doing so by excessively stringent restrictions on disclosure of protected health information to health care facilities' directories. Accordingly, the final rule takes an opt-out approach, stating that health care institutions may include the name, general condition, religious affiliation, and location of a patient within the facility in the facility's directory unless the patient explicitly objects to the use or disclosure of protected health information for directory purposes. To ensure that this opt-out can be exercised, the final rule requires facilities to notify individuals of their right not to be included in the directory and to give them the opportunity to opt out. The final rule indicates that the notice and opt-out may be oral. The final rule that allows health care facilities to disclose to clergy the four types of protected health information specified above without requiring the clergy to ask for the individual by name will allow the clergy to identify the members of his or her faith who are in the facility, thus ensuring that this rule will not significantly interfere with the exercise of religion, including the clergy's traditional religious mission to provide services to individuals.

Comment: A small number of commenters recommended requiring written authorization for all disclosures of protected health information for directory purposes. These commenters believed that the NPRM's proposed provision allowing oral agreement would not provide sufficient privacy protection; that it did not sufficiently hold providers accountable for complying with patient wishes; and that it could create liability issues for providers.

Response: The final rule does not require written authorization for disclosure of protected health information for directory purposes. We believe that requiring written authorization in these cases would increase substantially the administrative burdens and costs for covered health care providers and could lead to significant inconvenience for families and others attempting to locate individuals in health care institutions. Experience from the State of Maine suggests that requiring written authorization before patient information may be included in facility directories

can be disruptive for providers, families, clergy, and others.

Comment: Domestic violence organizations raised concerns that including information about domestic violence victims in health care facilities' directories could result in further harm to victims. The NPRM addressed the issue of potential danger to patients by stating that when patients were incapacitated, covered health care providers could exercise discretion—consistent with good medical practice and prior expression of patient preference—regarding whether to disclose protected health information for directory purposes. Several commenters recommended prohibiting providers from including information in a health care facility's directory about incapacitated individuals when the provider reasonably believed that the injuries to the individual could have been caused by domestic violence. These groups believed that such a prohibition was necessary to prevent abusers from locating and causing further harm to domestic violence patients.

Response: We share commenters' concerns about protecting victims of domestic violence from further abuse. We are also concerned, however, that imposing an affirmative duty on institutions not to disclose information any time injuries to the individual could have been the result of domestic violence would place too high a burden on health care facilities, essentially requiring them to rule out domestic violence as a potential cause of the injuries before disclosing to family members that an incapacitated person is in the institution.

We do believe, however, that it is appropriate to require covered health care providers to consider whether including the individual's name and location in the directory could lead to serious harm. As in the preamble to the NPRM, in the preamble to the final rule, we encourage covered health care providers to consider several factors when deciding whether to include an incapacitated patient's information in a health care facility's directory. One of these factors is whether disclosing an individual's presence in the facility could reasonably cause harm or danger to the individual (for example, if it appeared that an unconscious patient had been abused and disclosing that the individual is in the facility could give the attacker sufficient information to seek out the person and repeat the abuse). Under the final rule, when the opportunity to object to uses and disclosures for a facility's directory cannot practicably be provided due to an individual's incapacity or an emergency treatment circumstance, covered health care providers may use or disclose some or all of the protected health information that the rule allows to be included in the directory, if the disclosure is: (1) consistent with the individual's prior expressed preference, if known to the covered health care provider; and (2) in the individual's best interest, as determined by the covered health care provider in the exercise of professional judgement. The rule allows covered health care providers making decisions about incapacitated patients to include some portions of the patient's information (such as name) but not other information (such as location in the facility) to protect patient interests.

Section 164.510(b)—Uses and Disclosures for Involvement in the Individual's Care and Notification Purposes

Comment: A number of comments supported the NPRM's proposed approach, which would have allowed covered entities to disclose protected health information to the individual's next of kin, family members, or other close personal friends when the individual verbally agreed to the disclosure. These commenters agreed that the presumption should favor disclosures to the next of kin, and they believed that health care providers should encourage individuals to share genetic information and information about transmittable diseases with family members at risk. Others agreed with the general approach but suggested the individual's agreement be noted in the medical record. These commenters also supported the NPRM's proposed reliance on good professional practices and ethics to determine when disclosures should be made to the next of kin when the individual's agreement could not practicably be obtained.

A few commenters recommended that the individual's agreement be in writing for the protection of the covered entity and to facilitate the monitoring of compliance with the individual's wishes. These commenters were concerned that, absent the individual's written agreement, the covered entity would become embroiled in intra-family disputes concerning the disclosures. Others argued that the individual's authorization should be obtained for all disclosures, even to the next of kin.

One commenter favored disclosures to family members and others unless the individual actively objected, as long as the disclosure was consistent with sound professional practice. Others believed that no agreement by the individual was necessary unless sensitive medical information would be disclosed or unless the health care provider was aware of the individual's prior objection. These commenters recommended that good professional practice and ethics determine when disclosures were appropriate and that disclosure should relate only to the individual's current treatment. A health care provider organization said that the ethical and legal obligations of the medical professional alone should control in this area, although it believed the proposed rule was generally consistent with these obligations.

Response: The diversity of comments regarding the proposal on disclosures to family members, next of kin, and other persons, reflects a wide range of current practice and individual expectations. We believe that the NPRM struck the proper balance between the competing interests of individual privacy and the need that covered health care providers may have, in some cases, to have routine, informal conversations with an individual's family and friends regarding the individual's treatment.

We do not agree with the comments stating that all such disclosures should be made only with consent or with the individual's written authorization. The rule does not prohibit obtaining the agreement of the individual in writing; however, we believe that imposing a requirement for consent or written authorization in all cases for disclosures to individuals involved in a person's care would be unduly burdensome for all parties. In the final rule, we clarify the circumstances in which such disclosures are permissible. The rule allows covered entities to disclose to family members, other relatives, close personal friends of the individual, or any other person identified by the individual, the protected health information directly relevant to such person's involvement with the individual's care or payment related to the individual's health care. In addition, the final rule allows covered entities to use or disclose protected health information to notify, or assist in the notification of (including identifying or locating) a family member, a personal representative of the individual, or another person responsible for the care of the individual, of the individual's location, general condition, or death. The final rule includes separate provisions for situations in which the individual is present and for when the individual is not present at the time of disclosure. When the individual is present and can make his or her own decisions, a covered entity may disclose protected health information only if the covered entity: (1) Obtains the

individual's agreement to disclose to the third parties involved in the individual's care; (2) provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or (3) reasonably infers from the circumstances, based on the exercise of professional judgement, that the individual does not object to the disclosure. The final rule continues to permit disclosures in circumstances when the individual is not present or when the opportunity to agree or object to the use or disclosure cannot practicably be provided due to the individual's incapacity or an emergency circumstance. In such instances, covered entities may, in the exercise of professional judgement, determine whether the disclosure is in the individual's best interests and if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's health care.

As discussed in the preamble for this section, we do not intend to disrupt most covered entities' current practices with respect to informing family members and others with whom a patient has a close personal relationship about a patient's specific health condition when a patient is incapacitated due to a medical emergency and the family member or close personal friend comes to the covered entity to ask about the patient's condition. To the extent that disclosures to family members and others in these situations currently are allowed under state law and covered entities' own rules, § 164.510(b) allows covered entities to continue making them in these situations, consistent with the exercise of professional judgement as to the patient's best interest. As indicated in the preamble above, this section is not intended to provide a loophole for avoiding the rule's other requirements, and it is not intended to allow disclosures to a broad range of individuals, such as journalists who may be curious about a celebrity's health status.

Comments: A few comments supported the NPRM approach because it permitted the current practice of allowing someone other than the patient to pick up prescriptions at pharmacies. One commenter noted that this practice occurs with respect to 25–40% of the prescriptions dispensed by community retail pharmacies. These commenters strongly supported the proposal's reliance on the professional judgement of pharmacists in allowing others to pick up prescriptions for bedridden or otherwise incapacitated patients, noting that in most cases it would be impracticable to verify that the person was acting with the individual's permission. Two commenters requested that the rule specifically allow this practice. One comment opposed the practice of giving prescriptions to another person without the individual's authorization, because a prescription implicitly could disclose medical information about the individual.

Response: As stated in the NPRM, we intended for this provision to authorize pharmacies to dispense prescriptions to family or friends who are sent by the individual to the pharmacy to pick up the prescription. We believe that stringent consent or verification requirements would place an unreasonable burden on numerous transactions. In addition, such requirements would be contrary to the expectations and preferences of all parties to these transactions. Although prescriptions are protected health information under the rule, we believe that the risk to individual privacy in allowing this practice to continue is minimal. We agree with the suggestion that the final rule should state explicitly that pharmacies have the authority to operate in this manner. Therefore, we have added a sentence to § 164.510(b)(3) allowing covered entities to use professional judgement and experience with common practice to make reasonable inferences of an individual's best interest in allowing a person to act on the individual's behalf to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information. In such situations, as when making disclosures of protected health information about an individual who is not present or is unable to agree to such disclosures, covered entities should disclose only information which directly relates to the person's involvement in the individual's current health care. Thus, when dispensing a prescription to a friend who is picking it up on the patient's behalf, the pharmacist should not disclose unrelated health information about medications that the patient has taken in the past which could prove embarrassing to the patient.

Comment: We received a few comments that misunderstood the provision as addressing disclosures related to deceased individuals.

Response: We understand that use of the term next of kin in this section may cause confusion. To promote clarity in the final rule, we eliminate the term ''next of kin,'' as well as the term's proposed definition. In the final rule, we address comments on next of kin and the deceased in the section on disclosure of protected health information about deceased individuals in § 164.512(g).

Comments: A number of commenters expressed concern for the interaction of the proposed section with state laws. Some of these comments interpreted the NPRM's use of the term next of kin as referring to individuals with health care power of attorney and thus they believed that the proposed rule's approach to next of kin was inappropriately informal and in conflict with state law. Others noted that some state laws did not allow health care information to be disclosed to family or friends without consent or other authorization. One commenter said that case law may be evolving toward imposing a more affirmative duty on health care practitioners to inform next of kin in a variety of circumstances. One commenter noted that state laws may not define clearly who is considered to be the next of kin.

Response: The intent of this provision was not to interfere with or change current practice regarding health care powers of attorney or the designation of other personal representatives. Such designations are formal, legal actions which give others the ability to exercise the rights of or make treatment decisions related to individuals. While persons with health care powers of attorney could have access to protected health information under the personal representatives provision (§ 164.502(g)), and covered entities may disclose to such persons under this provision, such disclosures do not give these individuals substantive authority to act for or on behalf of the individual with respect to health care decisions. State law requirements regarding health care powers of attorney continue to apply.

The comments suggesting that state laws may not allow the disclosures otherwise permitted by this provision or, conversely, that they may impose a more affirmative duty, did not provide any specifics with which to judge the affect of such laws. In general, however, state laws that are more protective of an individual's privacy interests than the rule by prohibiting a disclosure of protected health information continue to apply. The rule's provisions regarding disclosure of protected health information to family or friends of the individual are permissive only, enabling covered entities to abide by more stringent state laws without violating our rules. Furthermore, if the state law creates an affirmative and binding legal obligation on the covered entity to make disclosures to family or other persons under specific circumstances, the final rule allows covered entities to comply

with these legal obligations. See § 164.512(a).

Comments: A number of commenters supported the proposal to limit disclosures to family or friends to the protected health information that is directly relevant to that person's involvement in the individual's health care. Some comments suggested that this standard apply to all disclosures to family or friends, even when the individual has agreed to or not objected to the disclosure. One commenter objected to the proposal, stating that it would be too difficult to administer. According to this comment, it is accepted practice for health care providers to communicate with family and friends about an individual's condition, regardless of whether the person is responsible for or otherwise involved in the individual's care.

Other comments expressed concern for disclosures related to particular types of information. For example, two commenters recommended that psychotherapy notes not be disclosed without patient authorization. One commenter suggested that certain sensitive medical information associated with social stigma not be disclosed to family members or others without patient consent.

Response: We agree with commenters who advocated limiting permissible disclosures to relatives and close personal friends to information consistent with a person's involvement in the individual's care. Under the final rule, we clarify the NPRM provision to state that covered entities may disclose protected health information to family members, relatives, or close personal friends of an individual or any other person identified by the individual, to the extent that the information directly relates to the person's involvement in the individual's current health care. It is not intended to allow disclosure of past medical history that is not relevant to the individual's current condition. In addition, as discussed above, we do not intend to disrupt covered entities' current practices with respect to disclosing specific information about a patient's condition to family members or others when the individual is incapacitated due to a medical emergency and the family member or other individual comes to the covered entity seeking specific information about the patient's condition. For example, this section allows a hospital to disclose to a family member the fact that a patient had a heart attack, and to provide updated information to the family member about the patient's progress and prognosis during his or her period of incapacity.

We agree with the recommendation to require written authorization for a disclosure of psychotherapy notes to family, close personal friends, or others involved in the individual's care. As discussed below, the final rule allows disclosure of psychotherapy notes without authorization in a few limited circumstances; disclosure to individuals involved in a person's care is not among those circumstances. See § 164.508 for a further discussion of the final rule's provisions regarding disclosure of psychotherapy notes.

We do not agree, however, with the suggestion to treat some medical information as more sensitive than others. In most cases, individuals will have the opportunity to prohibit or limit such disclosures. For situations in which an individual is unable to do so, covered entities may, in the exercise of professional judgement, determine whether the disclosure is in the individual's best interests and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's health care.

Comment: One commenter suggested that this provision should allow disclosure of protected health information to the clergy and to the Red Cross. The commenter noted that clergy have ethical obligations to ensure confidentiality and that the Red Cross often notifies the next of kin regarding an individual's condition in certain circumstances. Another commenter recommended allowing disclosures to law enforcement for the purpose of contacting the next of kin of individuals who have been injured or killed. One commenter sought clarification that ''close personal friend'' was intended to include domestic partners and same-sex couples in committed relationships.

Response: As discussed above, § 164.510(a) allows covered health care providers to disclose to clergy protected health information from a health care facility's directory. Under § 164.510(b), an individual may identify any person, including clergy, as involved in his or her care. This approach provides more flexibility than the proposed rule would have provided.

As discussed in the preamble of the final rule, this provision allows disclosures to domestic partners and others in same-sex relationships when such individuals are involved in an individual's care or are the point of contact for notification in a disaster. We do not intend to change current practices with respect to involvement of others in an individual's treatment decisions; informal information-sharing among persons involved; or the sharing of protected health information during a disaster. As noted above, a power of attorney or other legal relationship to an individual is not necessary for these informal discussions about the individual for the purpose of assisting in or providing a service related to the individual's care.

We agree with the comments noting that the Red Cross and other organizations may play an important role in locating and communicating with the family about individuals injured or killed in an accident or disaster situation. Therefore, the final rule includes new language, in § 164.510(b)(4), which allows covered entities to use or disclose protected health information to a public or private entity authorized by law or its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities to notify, or assist in the notification of (including identifying or locating) a family member, an individual's personal representative, or another person responsible for the individual's care regarding the individual's location, general condition, or death. The Red Cross is an example of a private entity that may obtain protected health information pursuant to these provisions. We recognize the role of the Red Cross and similar organizations in disaster relief efforts, and we encourage cooperation with these entities in notification efforts and other means of assistance.

Comment: One commenter recommended stating that individuals who are mentally retarded and unable to agree to disclosures under this provision do not, thereby, lose their access to further medical treatment. This commenter also proposed stating that mentally retarded individuals who are able to provide agreement have the right to control the disclosure of their protected health information. The commenter expressed concern that the parent, relative, or other person acting *in loco parentis* may not have the individual's best interest in mind in seeking or authorizing for the individual the disclosure of protected health information.

Response: The final rule regulates only uses and disclosures of protected health information, not the delivery of health care. Under the final rule's section on personal representatives (§ 164.502(g)), a person with authority to make decisions about the health care of an individual, under applicable law, may make decisions about the protected health information of that individual, to the extent that the protected health information is relevant to such person's representation.

In the final rule, § 164.510(b) may apply to permit disclosures to a person other than a personal representative. Under § 164.510(b), when an individual is present and has the capacity to make his or her own decisions, a covered entity may disclose protected health information only if the covered entity: (1) Obtains the individual's agreement to disclose protected health information to the third parties involved in the individual's care; (2) provides the individual with an opportunity to object to such disclosure, and the individual does not express an objection; or (3) reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure. These conditions apply to disclosure of protected health information about individuals with mental retardation as well as to disclosures about all other individuals. Thus we do not believe it is necessary to include in this section of the final rule any language specifically on persons with mental retardation.

Comments: A few commenters recommended that disclosures made in good faith to the family or friends of the individual not be subject to sanctions by the Secretary, even if the covered entity had not fully complied with the requirements of this provision. One commenter believed that a fear of sanction would make covered entities overly cautious, such that they would not disclose protected health information to domestic partners or others not recognized by law as next of kin. Another commenter recommended that sanctions not be imposed if the covered entity has proper policies in place and has trained its staff appropriately. According to this commenter, the lack of documentation of disclosures in a particular case or medical record should not subject the entity to sanctions if the information was disclosed in good faith.

Response: We generally agree with commenters regarding disclosure in good faith pursuant to this provision. As discussed above, the final rule expands the scope of individuals to whom covered entities may disclose protected health information pursuant to this section. In addition, we delete the term next of kin, to avoid the appearance of requiring any legal determination of a person's relationship in situations involving informal disclosures. Similarly, consistent with the informal nature of disclosures pursuant to this section, we do not require covered entities to document such disclosures. If a covered entity imposes its own documentation requirements and a particular covered health care provider does not follow the entity's documentation requirements, the disclosure is not a violation of this rule.

Comments: The majority of comments on this provision were from individuals and organizations concerned about domestic violence. Most of these commenters wanted assurance that domestic violence would be a consideration in any disclosure to the spouse or relatives of an individual whom the covered entity suspected to be a victim of domestic violence or abuse. In particular, these commenters recommended that disclosures not be made to family members suspected of being the abuser if to do so would further endanger the individual. Commenters believed that this limitation was particularly important when the individual was unconscious or otherwise unable to object to the disclosures.

Response: We agree with the comments that victims of domestic violence and other forms of abuse need special consideration in order to avoid further harm, and we provide for discretion of a covered entity to determine that protected health information not be disclosed pursuant to § 164.510(b). Section 164.510(b) of the final rule, disclosures to family or friends involved in the individual's care, states that when an individual is unable to agree or object to the disclosure due to incapacity or another emergency situation, a covered entity must determine based on the exercise of professional judgment whether it is in the individual's best interest to disclose the information. As stated in the preamble, we intend for this exercise of professional judgment in the individual's best interest to account for the potential for harm to the individual in cases involving domestic violence. These circumstances are unique and are best decided by a covered entity, in the exercise of professional judgment, in each situation rather than by a blanket rule.

Section 164.512—Uses and Disclosures for Which Consent, Authorization, or Opportunity to Agree or Object Is Not Required

Section 164.512(a)—Uses and Disclosures Required by Law

Comment: Numerous commenters addressed directly or by implication the question of whether the provision permitting uses and disclosures of protected health information if required by other law was necessary. Other commenters generally endorsed the need for such a provision. One such commenter approved of the provision as a needed fail-safe mechanism should the enumeration of permissible uses and disclosures of protected health information in the NPRM prove to be incomplete. Other commenters cited specific statutes which required access to protected health information, arguing that such a provision was necessary to ensure that these legally mandated disclosures would continue to be permitted. For example, some commenters argued for continued access to protected health information to investigate and remedy abuse and neglect as currently required by the Developmental Disabilities Assistance and Bill of Rights, 42 U.S.C. 6042, and the Protection and Advocacy for Mentally Ill Individuals Act, 42 U.S.C. 10801.

Some comments urged deletion of the provision for uses and disclosures required by other law. This concern appeared to be based on a generalized concern that the provision fostered government intrusion into individual medical information.

Finally, a number of commenters also urged that the required by law provision be deleted. These commenters argued that the proposed provision would have undermined the intent of the statute to preempt state laws which were less protective of individual privacy. As stated in these comments, the provision for uses and disclosures required by other law was ''broadly written and could apply to a variety of state laws that are contrary to the proposed rule and less protective of privacy. (Indeed, a law *requiring* disclosure is the least protective of privacy since it allows for no discretion.) The breadth of this provision greatly exceeds the exceptions to preemption contained in HIPAA.''

Response: We agree with the comments that proposed § 164.510(n) was necessary to harmonize the rule with existing state and federal laws mandating uses and disclosures of protected health information. Therefore, in the final rule, the provision permitting uses and disclosures as required by other law is retained. To accommodate other reorganization of the final rule, this provision has been designated as § 164.512(a).

We do not agree with the comments expressing concern for increased governmental intrusion into individual privacy under this provision. The final rule does not create any new duty or obligation to disclose protected health information. Rather, it permits covered entities to use or disclose protected health information when they are required by law to do so.

We likewise disagree with the characterization of the proposed provision as inconsistent with or contrary to the preemption standards in the statute or Part 160 of the rule. As described in the NPRM, we intend this provision to preserve access to information considered important enough by state or federal authorities to require its disclosure by law.

The importance of these required uses or disclosures is evidenced by the legislative or other public process necessary for the government to create a legally binding obligation on a covered entity. Furthermore, such required uses and disclosures arise in a myriad of other areas of law, ranging from topics addressing national security (uses and disclosures to obtain security clearances), to public health (reporting of communicable diseases), to law enforcement (disclosures of gun shot wounds). Required uses and disclosures also may address broad national concerns or particular regional or state concerns. It is not possible, or appropriate, for HHS to reassess the legitimacy of or the need for each of these mandates in each of their specialized contexts. In some cases where particular concerns have been raised by legal mandates in other laws, we allow disclosure as required by law, and we establish additional requirements to protect privacy (for example, informing the individual as required in § 164.512(c)) when covered entities make a legally mandated disclosure.

We also disagree with commenters who suggest that the approach in the final rule is contrary to the preemption provisions in HIPAA. HIPAA provides HHS with broad discretion in fashioning privacy protections. Recognizing the legitimacy of existing legal requirements is certainly within the Secretary's discretion. Additionally, given the variety of these laws, the varied contexts in which they arise, and their significance in ensuring that important public policies are achieved, we do not believe that Congress intended to preempt each such law unless HHS specifically recognized the law or purpose in the regulation.

Comment: A number of commenters urged that the provision permitting uses and disclosures required by other law be amended by deleting the last sentence which stated: ''This paragraph does not apply to uses or disclosures that are covered by paragraphs (b) through (m) of this section.'' Some commenters sought deletion of this sentence to avoid any inadvertent preemption of mandatory reporting laws, and requested clarification of the effect on specific statutes.

The majority of the commenters focused their concerns on the potential conflict between mandatory reporting laws to law enforcement and the limitations imposed by proposed § 164.510(f), on uses and disclosures to law enforcement. For example, the comments raised concerns that mandatory reporting to law enforcement of injuries resulting from violent acts and abuse require the health care provider to initiate such reports to local law enforcement or other state agencies, while the NPRM would have allowed such reporting on victims of crimes only in response to specific law enforcement requests for information. Similarly, mandatory reports of violence-related injuries may implicate suspected perpetrators, as well as victims, and compliance with such laws could be blocked by the proposed requirement that disclosures about suspects was similarly limited to a response to law enforcement inquiries for the specific purpose of identifying the suspect. The NPRM also would have limited the type of protected health information that could have been disclosed about a suspect or fugitive.

In general, commenters sought to resolve this overlap by removing the condition that the required-by-other-law provision applied only when no other national priority purpose addressed the particular use or disclosure. The suggested change would permit the covered entity to comply with legally mandated uses and disclosures as long as the relevant requirements of that law were met. Alternatively, other commenters suggested that the restrictions on disclosures to law enforcement be lifted to permit full compliance with laws requiring reporting for these purposes.

Finally, some comments sought clarification of when a use or disclosure was ''covered by paragraphs (b) through (m).'' These commenters were confused as to whether a particular use or disclosure had to be specifically addressed by another provision of the rule or simply within the scope of the one of the national priority purposes specified by proposed paragraphs (b) through (m).

Response: We agree with the commenters that the provision as proposed would have inadvertently interfered with many state and federal laws mandating the reporting to law enforcement or others of protected health information.

In response to these comments, we have modified the final rule to clarify how this section interacts with the other provisions in the rule.

Comment: A number of commenters sought expanded authority to use and disclosure protected health information when permitted by other law, not just when required by law. These comments specified a number of significant duties or potential societal benefits from disclosures currently permitted or authorized by law, and they expressed concern should these beneficial uses and disclosures no longer be allowed if not specifically recognized by the rule. For example, one commenter listed 25 disclosures of health records that are currently permitted, but not required, by state law. This commenter was concerned that many of these authorized uses and disclosures would not be covered by any of the national priority purposes specified in the NPRM, and, therefore, would not be a permissible use or disclosure under the rule. To preserve these important uses and disclosures, the comments recommended that provision be made for any use or disclosure which is authorized or permitted by other law.

Response: We do not agree with the comments that seek general authority to use and disclose protected health information as permitted, but not required, by other law. The uses and disclosures permitted in the final rule reflect those purposes and circumstances which we believe are of sufficient national importance or relevance to the needs of the health care system to warrant the use or disclosure of protected health information in the absence of either the individual's express authorization or a legal duty to make such use or disclosure. In permitting specific uses and disclosures that are not required by law, we have considered the individual privacy interests at stake in each area and crafted conditions or limitations in each identified area as appropriate to balance the competing public purposes and individual privacy needs. A general rule authorizing any use or disclosure that is permitted, but not required, by other law would undermine the careful balancing in the final rule.

In making this judgment, we have distinguished between laws that mandate uses or disclosures and laws that merely permit them. In the former case, jurisdictions have determined that public policy purposes cannot be achieved absent the use of certain protected health information, and we have chosen in general not to disturb their judgments. On the other hand, where jurisdictions have determined that certain protected health information is not necessary to achieve

a public policy purpose, and only have permitted its use or disclosure, we do not believe that those judgments reflect an interest in use or disclosure strong enough to override the Congressional goal of protecting privacy rights.

Moreover, the comments failed to present any compelling circumstance to warrant such a general provision. Despite commenters' concerns to the contrary, most of the beneficial uses and disclosures that the commenters referenced to support a general provision were, in fact, uses or disclosures already permissible under the rule. For example, the general statutory authorities relied on by one state health agency to investigate disease outbreaks or to comply with health data-gathering guidelines for reporting to certain federal agencies are permissible disclosures to public health agencies.

Finally, in the final rule, we add new provisions to § 164.512 to address three examples raised by commenters of uses and disclosures that are authorized or permitted by law, but may not be required by law. First, commenters expressed concern for the states that provide for voluntary reporting to law enforcement or state protective services of domestic violence or of abuse, neglect or exploitation of the elderly or other vulnerable adults. As discussed below, a new section, § 164.512(c), has been added to the final rule to specifically address uses and disclosures of protected health information in cases of abuse, neglect, or domestic violence. Second, commenters were concerned about state or federal laws that permitted coordination and cooperation with organizations or entities involved in cadaveric organ, eye, or tissue donation and transplantation. In the final rule, we add a new section, § 164.512(h), to permit disclosures to facilitate such donation and transplantation functions. Third, a number of commenters expressed concern for uses and disclosure permitted by law in certain custodial settings, such as those involving correctional or detention facilities. In the final rule, we add a new subsection to the section on uses and disclosures for specialized government functions, § 164.512(k), to identify custodial settings in which special rules are necessary and to specify the additional uses and disclosures of the protected health information of inmates or detainees which are necessary in such facilities.

Comment: A number of commenters asked for clarification of the term ''law'' and the phrase ''required by law'' for purposes of the provision permitting uses or disclosures that are required by law. Some of the commenters noted that ''state law'' was a defined term in Part 160 of the NPRM and that the terms should be used consistently. Other commenters were concerned about differentiating between laws that required a use or disclosure and those that merely authorize or permit a use or disclosure. A number of commenters recommended that the final rule include a definitive list of the laws that mandate a use or disclosure of protected health information.

Response: In the final rule, we clarify that, consistent with the ''state law'' definition in § 160.202, ''law'' is intended to be read broadly to include the full array of binding legal authority, such as constitutions, statutes, rules, regulations, common law, or other governmental actions having the effect of law. However, for the purposes of § 164.512(a), law is not limited to state action; rather, it encompasses federal, state or local actions with legally binding effect, as well as those by territorial and tribal governments.

For more detail on the meaning of ''required by law,'' see § 164.501. Only where the law imposes a duty on the health care professional to report would the disclosure be considered to be required by law.

The final rule does not include a definitive list of the laws that contain legal mandates for disclosures of protected health information. In light of the breadth of the term ''law'' and number of federal, state, local, and territorial or tribal authorities that may engage in the promulgation of binding legal authority, it would be impossible to compile and maintain such a list. Covered entities have an independent duty to be aware of their legal obligations to federal, state, local and territorial or tribal authorities. The rule's approach is simply intended to avoid any obstruction to the health plan or covered health care provider's ability to comply with its existing legal obligations.

Comment: A number of commenters recommended that the rule compel covered entities to use or disclose protected health information as required by law. They expressed concern that covered entities could refuse or delay compliance with legally mandated disclosures by misplaced reliance on a rule that permits, but does not require, a use or disclosure required by other law.

Response: We do not agree that the final rule should require covered entities to comply with uses or disclosures of protected health information mandated by law. The purpose of this rule is to protect privacy, and to allow those disclosures consistent with sound public policy. Consistent with this purpose, we mandate disclosure only to the individual who is the subject of the information, and for purposes of enforcing the rule. Where a law imposes a legal duty on the covered entity to use or disclose protected health information, it is sufficient that the privacy rule permit the covered entity to comply with such law. The enforcement of that legal duty, however, is a matter for that other law.

Section 164.512(b)—Uses and Disclosures for Public Health Activities

Comment: Several non-profit entities commented that medical records research by nonprofit entities to ensure public health goals, such as disease-specific registries, would not have been covered by this provision. These organizations collect information without relying on a government agency or law. Commenters asserted that such activities are essential and must continue. They generally supported the provisions allowing the collection of individually identifiable health information without authorization for registries. One stated that both governmental and non-governmental cancer registries should be exempt from the regulation. They stated that ''such entities, by their very nature, collect health information for legitimate public health and research purposes.'' Another, however, addressed its comments only to ''disclosure to non-government entities operating such system as required or authorized by law.''

Response: We acknowledge that such entities may be engaged in disease-specific or other data collection activities that provide a benefit to their members and others affected by a particular malady and that they contribute to the public health and scientific database on low incidence or little known conditions. However, in the absence of some nexus to a government public health authority or other underlying legal authority, it is unclear upon what basis covered entities can determine which registries or collections are ''legitimate'' and how the confidentiality of the registry information will be protected. Commenters did not suggest methods for ''validating'' these private registry programs, and no such methods currently exist at the federal level. It is unknown whether any states have such a program. Broadening the exemption could provide a loophole for private data collections for inappropriate

purposes or uses under a ''public health'' mask.

In this rule, we do not seek to make judgments as to the legitimacy of private entities' disease-specific registries or of private data collection endeavors. Rather, we establish the general terms and conditions for disclosure and use of protected health information. Under the final rule, covered entities may obtain authorization to disclose protected health information to private entities seeking to establish registries or other databases; they may disclose protected health information as required by law; or they may disclose protected health information to such entities if they meet the conditions of one of the provisions of §§ 164.510 or 164.512. We believe that the circumstances under which covered entities may disclose protected health information to private entities should be limited to specified national priority purposes, as reflected through the FDA requirements or directives listed in § 164.512(b)(iii), and to enable recalls, repairs, or replacements of products regulated by the FDA. Disclosures by covered health care providers who are workforce members of an employer or are conducting evaluations relating to work-related injuries or illnesses or workplace surveillance also may disclose protected health information to employers of findings of such evaluations that are necessary for the employer to comply with requirements under OSHA and related laws.

Comment: Several commenters said that the NPRM did not indicate how to distinguish between public health data collections and government health data systems. They suggested eliminating proposed § 164.510(g) on disclosures and uses for government health data systems, because they believed that such disclosures and uses were adequately covered by proposed § 164.510(b) on public health.

Response: As discussed below, we agree with the commenters who suggested that the proposed provision that would have permitted disclosures to government health data bases was overly broad, and we remove it from the final rule. We reviewed the important purposes for which some commenters said government agencies needed protected health information, and we believe that most of those needs can be met through the other categories of permitted uses and disclosures without authorization allowed under the final rule, including provisions permitting covered entities to disclose information (subject to certain limitations) to government agencies for public health, health oversight, law enforcement, and otherwise as required by law. For example, the final rule continues to allow collection of protected health information without authorization to monitor trends in the spread of infectious disease, morbidity and mortality.

Comment: Several commenters recommended expanding the scope of disclosures permissible under proposed § 164.510(b)(1)(iii), which would have allowed covered entities to disclose protected health information to private entities that could demonstrate that they were acting to comply with requirements, or at the direction, of a public health authority. These commenters said that they needed to collect individually identifiable health information in the process of drug and device development, approval, and post-market surveillance—activities that are related to, and necessary for, the FDA regulatory process. However, they noted that the specific data collections involved were not required by FDA regulations. Some commenters said that they often devised their own data collection methods, and that health care providers disclosed information to companies voluntarily for activities such as post-marketing surveillance and efficacy surveys. Commenters said they used this information to comply with FDA requirements such as reporting adverse events, filing other reports, or recordkeeping. Commenters indicated that the FDA encouraged but did not require them to establish other data collection mechanisms, such as pregnancy registries that track maternal exposure to drugs and the outcomes.

Accordingly, several commenters recommended modifying proposed § 164.510(b) to allow covered entities to disclose protected health information without authorization to manufacturers registered with the FDA to manufacture, distribute, or sell a prescription drug, device, or biological product, in connection with post-marketing safety and efficacy surveillance or for the entity to obtain information about the drug, device, or product or its use. One commenter suggested including in the regulation an illustrative list of examples of FDA-related requirements, and stating in the preamble that all activities taken in furtherance of compliance with FDA regulations are ''public health activities.''

Response: We recognize that the FDA conducts or oversees many activities that are critical to help ensure the safety or effectiveness of the many products it regulates. These activities include, for example, reporting of adverse events, product defects and problems; product tracking; and post-marketing surveillance. In addition, we believe that removing defective or harmful products from the market is a critical national priority and is an important tool in FDA efforts to promote the safety and efficacy of the products it regulates. We understand that in most cases, the FDA lacks statutory authority to require product recalls. We also recognize that the FDA typically does not conduct recalls, repairs, or product replacement surveillance directly, but rather, that it relies on the private entities it regulates to collect data, notify patients when applicable, repair and replace products, and undertake other activities to promote the safety and effectiveness of FDA-regulated products.

We believe, however, that modifying the NPRM to allow disclosure of protected health information to private entities as part of any data-gathering activity related to a drug, device, or biological product or its use, or for any activity that is consistent with, or that appears to promote objectives specified, in FDA regulation would represent an inappropriately broad exception to the general requirement to obtain authorization prior to disclosure. Such a change could allow, for example, drug companies to collect protected health information without authorization to use for the purpose of marketing pharmaceuticals. We do not agree that all activities taken to promote compliance with FDA regulations represent public health activities as that term is defined in this rule. In addition, we believe it would not be appropriate to include in the regulation text an ''illustrative list'' of requirements ''related to'' the FDA. The regulation text and preamble list the FDA-related activities for which we believe disclosure of protected health information to private entities without authorization is warranted.

We believe it is appropriate to allow disclosure of protected health information without authorization to private entities only: For purposes that the FDA has, in effect, identified as national priorities by issuing regulations or express directions requiring such disclosure; or if such disclosure is necessary for a product recall. For example, we believe it is appropriate to allow covered health care providers to disclose to a medical device manufacturer recalling defective heart valves the names and last known addresses of patients in whom the provider implanted the valves. Thus, in the final rule, we allow covered entities to disclose protected health information to entities subject to FDA jurisdiction for the following activities: To report adverse events (or similar reports with

respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations, if the disclosure is made to the person required or directed to report such information to the FDA; to track products if the disclosure is made to a person required or directed by the FDA to track the product; to enable product recalls, repairs, or replacement (including locating and notifying individuals who have received products of product recalls, withdrawals, or other problems); or to conduct post-marketing surveillance to comply with requirements or at the direction of the FDA. The preamble above provides further detail on the meaning of some of the terms in this list. Covered entities may disclose protected health information to entities for activities other than those described above only as required by law; with authorization; or if permissible under another section of this rule.

We understand that many private registries, such as pregnancy registries, currently obtain patient authorization for data collection. We believe the approach of § 164.512(b) strikes an appropriate balance between the objective of promoting patient privacy and control over their health information and the objective of allowing private entities to collect data that ultimately may have important public health benefits.

Comment: One commenter remarked that our proposal may impede fetal/infant mortality and child fatality reviews.

Response: The final rule permits a covered entity to disclose protected health information to a public health authority authorized by law to conduct public health activities, including the collection of data relevant to death or disease, in accordance with § 164.512(b). Such activities may also meet the definition of ''health care operations.'' We therefore do not believe this rule impedes these activities.

Comment: Several comments requested that the final regulation clarify that employers be permitted to use and/or disclose protected health information pursuant to the requirements of the Occupational Safety and Health Act and its accompanying regulations (''OSHA''). A few comments asserted that the regulation should not only permit employers to use and disclose protected health information without first obtaining an authorization consistent with OSHA requirements, but also permit them to use and disclose protected health information if the use or disclosure is consistent with the spirit of OSHA. One commenter supported the permissibility of these types of uses and disclosures, but warned that the regulation should not grant employers unfettered access to the entire medical record of employees for the purpose of meeting OSHA requirements. Other commenters noted that OSHA not only requires disclosures to the Occupational Safety and Health Administration, but also to third parties, such as employers and employee representatives. Thus, this comment asked HHS to clarify that disclosures to third parties required by OSHA are also permissible under the regulation.

Response: Employers as such are not covered entities under HIPAA and we generally do not have authority over their actions. When an employer has a health care component, such as an on-site medical clinic, and the components meets the requirements of a covered health care provider, health plan or health care clearinghouse, the uses and disclosures of protected health information by the health care component, including disclosures to the larger employer entity, are covered by this rule and must comply with its provisions.

A covered entity, including a covered health care provider, may disclose protected health information to OSHA under § 164.512(a), if the disclosure is required by law, or if the disclosure is a discretionary one for public health activities, under § 164.512(b). Employers may also request employees to provide authorization for the employer to obtain protected health information from covered entities to conduct analyses of work-related health issues. See § 164.508.

We also permit covered health care providers who provide health care as a workforce member of an employer or at the request of an employer to disclose protected health information to the employer concerning work-related injuries or illnesses or workplace medical surveillance in situations where the employer has a duty to keep records on or act on such information under the OSHA or similar laws. We added this provision to ensure that employers are able to obtain the information that they need to meet federal and state laws designed to promote safer and healthier workplaces. These laws are vital to protecting the health and safety of workers and we permit specified covered health care providers to disclose protected health information as necessary to carry out these purposes.

Comment: A few comments suggested that the final regulation clarify how it would interact with existing and pending OSHA requirements. One of these comments requested that the Secretary delay the effective date of the regulation until reviews of existing requirements are complete.

Response: As noted in the ''Relationship to Other Federal Laws'' section of the preamble, we are not undertaking a complete review of all existing laws with which covered entities might have to comply. Instead we have described a general framework under which such laws may be evaluated. We believe that adopting national standards to protect the privacy of individually identifiable health information is an urgent national priority. We do not believe that it is appropriate to delay the effective date of this regulation.

Comment: One commenter asserted that the proposed regulation conflicted with the OSHA regulation requirement that when a designated representative (to whom the employee has already provided a written authorization to obtain access) requests a release form for access to employee medical records, the form must include the purpose for which the disclosure is sought, which the proposed privacy regulation does not require.

Response: We do not agree that this difference creates a conflict for covered entities. If an employer seeks to obtain a valid authorization under § 164.508, it may add a purpose statement to the authorization so that it complies with OSHA's requirements and is a valid authorization under § 164.508 upon which a covered entity may rely to make a disclosure of protected health information to the employer.

Comment: One commenter stated that access to workplace medical records by the occupational medical physicians is fundamental to workplace and community health and safety. Access is necessary whether it is a single location or multiple sites of the same company, such as production facilities of a national company located throughout the country.

Response: We permit covered health care providers who provide health care as a workforce member of an employer or at the request of an employer to disclose protected health information to the employer concerning work-related injuries or illnesses or workplace medical surveillance, as described in this paragraph. Information obtained by an employer under this paragraph would be available for it to use, consistent with other laws and regulations, as it chooses and throughout the national company. We do not regulate uses or disclosures of individually identifiable health

information by employers acting as employers.

Section 164.512(c)—Disclosures About Victims of Abuse, Neglect, or Domestic Violence

The NPRM did not include a paragraph specifically addressing covered entities' disclosures of protected health information regarding victims of abuse, neglect, or domestic violence. Rather, the NPRM addressed disclosures about child abuse pursuant to proposed § 164.510(b), which would have allowed covered entities to report child abuse to a public health authority or to another appropriate authority authorized by law to receive reports of child abuse or neglect. We respond to comments regarding victims of domestic violence or abuse throughout the final rule where relevant. (See responses to comments on §§ 164.502(g), 164.510(b), 164.512(f)(3), 164.522, and 164.524.)

Comment: Several commenters urged us to require that victims of domestic violence be notified about requests for or disclosures of protected health information about them, so that victims could take safety precautions.

Response: We agree that, in balancing the burdens on covered entities from such a notification requirement against the benefits to be gained, victims of domestic abuse merit heightened concern. For this reason, we generally require covered entities to inform the individual when they disclose protected health information to authorized government authorities. As the Family Violence Prevention Fund has noted in its *Health Privacy Principles for Protecting Victims of Domestic Violence* (October 2000), victims of domestic violence and abuse sometimes are subject to retaliatory violence. By informing a victim of abuse or domestic violence of a disclosure to law enforcement or other authorities, covered entities give victims the opportunity to take appropriate safety precautions. See the above preamble discussion of § 164.512(c) for more detail about the requirements for disclosing protected health information about victims of domestic violence.

Comment: Some commenters argued that a consent requirement should apply at a minimum to disclosures involving victims of crime or victims of domestic violence.

Response: We agree, and we modify the proposed rule to require covered entities to obtain an individual's agreement prior to disclosing protected health information in most instances involving victims of a crime or of abuse, neglect, or domestic violence. See the above preamble discussions of § 164.512(c), on disclosures about victims of abuse, neglect, or domestic violence, and § 164.512(f)(3), on disclosures to law enforcement about crime victims.

Section 164.512(d)—Uses and Disclosures for Health Oversight Activities

Comment: A couple of commenters supported the NPRM's approach to health oversight. Several other commenters generally supported the NPRM's approach to disclosure of protected health information for national priority purposes, and they recommended some clarification regarding disclosure for health oversight. Two commenters recommended clarifying in the final rule that disclosure is allowed to all federal, state, and local agencies that use protected health information to carry out legally mandated responsibilities.

Response: The final rule permits disclosures to public agencies that meet the definition of a health oversight agency and for oversight of the particular areas described in the statute. Section 164.512(a) of the final rule permits disclosures that are required by law. As discussed in the responses to comments of § 164.512(a), we do not in the final rule permit disclosures merely authorized by other laws that do not fit within the other public policy purposes recognized by the rule.

Comment: One commenter recommended clarifying in the final rule that covered entities are not required to establish business partner contracts with health oversight agencies or public health authorities to release individually identifiable information to them for purposes exempt from HIPAA and sanctioned by state law.

Response: The final rule does not require covered entities to establish business associate contracts with health oversight agencies when they disclose protected health information to these agencies for oversight purposes.

Comment: Two commenters recommended clarifying in the regulation text that the health oversight section does not create a new right of access to protected health information.

Response: We agree and include such a statement in the preamble of § 164.512(d) of the final rule.

Comment: Several commenters were concerned that the proposed oversight section allowed but did not require disclosure of protected health information to health oversight agencies for oversight activities.

Response: This rule's purpose is to protect the privacy of individually identifiable health information. Except to enforce the rule and to establish individuals' right to access their own protected health information (see § 164.502(a)(2)), we do not require disclosure of protected health information to any person or entity. We allow such disclosure for situations in which other laws require disclosure.

Comment: Some commenters were concerned that the NPRM would have allowed health oversight agencies to re-use and redisclose protected health information to other entities, and they were particularly concerned about re-disclosure to and re-use by law enforcement agencies. One commenter believed that government agencies would use the label of health oversight to gain access to protected health information from covered entities—thereby avoiding the procedural requirements of the law enforcement section (proposed § 164.510(f)) and subsequently would turn over information to law enforcement officials. Thus, these groups were concerned that the potential for oversight access to protected health information under the rule to become the ''back door'' to law enforcement access to such information.

Based on their concerns, these commenters recommended establishing a general prohibition on the re-use and re-disclosure of protected health information obtained by health oversight agencies in actions against individuals. One health plan expressed general concern about re-disclosure among all of the public agencies covered in the proposed § 164.510. It recommended building safeguards into the rule to prevent information gathered for one purpose (for example, public health) from being used for another purpose (such as health oversight).

Many of the commenters concerned about re-disclosure of protected health information obtained for oversight purposes said that if the Secretary lacked statutory authority to regulate oversight agencies' re-disclosure of protected health information and the re-use of this information by other agencies covered in proposed § 164.510, the President should issue an Executive Order barring such re-disclosure and re-use. One of these groups specified that the Executive Order should bar re-use and re-disclosure of protected health information in actions against individuals.

In contrast, some commenters advocated information-sharing between law enforcement and oversight agencies. Most of these commenters recognized that the NPRM would have allowed re-use and re-disclosure of protected health information from oversight to law

enforcement agencies, and they supported this approach.

Response: We believe that the language we have added to the rule, at § 164.512(d)(2) and the corresponding explanation in the preamble, to clarify the boundary between disclosures for health oversight and for law enforcement purposes should partially address the concern expressed by some that oversight agencies will be the back door for access by law enforcement. In situations when the individual is the subject of an investigation or activity and the investigation or activity is not related to health care fraud, the requirements for disclosure to law enforcement must be met, and an oversight agency cannot request the information under its more general oversight authority.

We acknowledge, however, that there will be instances under the rule when a health oversight agency (or a law enforcement agency in its oversight capacity) that has obtained protected health information appropriately will be able to redisclose the information to a law enforcement agency for law enforcement purposes. Under HIPAA, we have the authority to restrict re-disclosure of protected health information only by covered entities. Re-disclosures by public agencies such as oversight agencies are not within the purview of this rule. We support the enactment of comprehensive privacy legislation that would govern such public agencies' re-use and re-disclosure of this information. Furthermore, in an effort to prevent health oversight provisions from becoming the back door to law enforcement access to protected health information, the President is issuing an Executive Order that places strict limitations on the use of protected health information gathered in the course of an oversight investigation for law enforcement activities. For example, such use will be subject to review by the Deputy Attorney General.

Comment: Several commenters recommended modifying the proposed oversight section to require health oversight officials to justify and document their need for identifiable information.

Response: We encourage covered entities to work with health oversight agencies to determine the scope of information needed for health oversight inquiries. However, we believe that requiring covered entities to obtain extensive documentation of health oversight information needs could compromise health oversight agencies' ability to complete investigations, particularly when an oversight agency is investigating the covered entity from which it is seeking information.

Comment: Several commenters believed that health oversight activities could be conducted without access to individually identifiable health information. Some of these groups recommended requiring information provided to health oversight agencies to be de-identified to the extent possible.

Response: We encourage health oversight agencies to use de-identified information whenever possible to complete their investigations. We recognize, however, that in some cases, health oversight agencies need identifiable information to complete their investigations. For example, as noted in the preamble to the NPRM, to determine whether a hospital has engaged in fraudulent billing practices, it may be necessary to examine billing records for a set of individual cases. Similarly, to determine whether a health plan is complying with federal or state health care quality standards, it may be necessary to examine individually identifiable health information in comparison with such standards. Thus, to allow health oversight agencies to conduct the activities that are central to their mission, the final rule does not require covered entities to de-identify protected health information before disclosing it to health oversight organizations.

Comment: One commenter recommended requiring whistleblowers, pursuant to proposed § 164.518(a)(4) of the NPRM, to raise the issue of a possible violation of law with the affected covered entity before disclosing such information to an oversight agency, attorney, or law enforcement official.

Response: We believe that such a requirement would be inappropriate, because it would create the potential for covered entities that are the subject of whistleblowing to take action to evade law enforcement and oversight action.

Comment: One commenter recommended providing an exemption from the proposed rule's requirements for accounting for disclosures when such disclosures were for health oversight purposes.

Response: We recognize that in some cases, informing individuals that their protected health information has been disclosed to a law enforcement official or to a health oversight agency could compromise the ability of law enforcement and oversight officials to perform their duties appropriately. Therefore, in the final rule, we retain the approach of proposed § 164.515 of the NPRM. Section 164.528(a)(2) of the final rule states that an individual's right to receive an accounting of disclosures to a health oversight agency, law enforcement official, or for national security or intelligence purposes may be temporarily suspended for the time specified by the agency or official. As described in § 164.528(a)(2), for such a suspension to occur, the agency or official must provide the affected covered entity with a written request stating that an accounting to the individual would be reasonably likely to impede the agency's activity. The request must specify the time for which the suspension is required. We believe that providing a permanent exemption to the right to accounting for disclosures for health oversight purposes would fail to ensure that individuals are sufficiently informed about the extent of disclosures of their protected health information.

Comment: One commenter recommended making disclosures to health oversight agencies subject to a modified version of the NPRM's proposed three-part test governing disclosure of protected health information to law enforcement pursuant to an administrative request (as described in proposed § 164.510(f)(1)).

Response: We disagree that it would be appropriate to apply the procedural requirements for law enforcement to health oversight. We apply more extensive procedural requirements to law enforcement disclosures than to disclosures for health oversight because we believe that law enforcement investigations more often involve situations in which the individual is the subject of the investigation (and thus could suffer adverse consequences), and we believe that it is appropriate to provide greater protection to individuals in such cases. Health oversight involves investigations of institutions that use health information as part of business functions, or of individuals whose health information has been used to obtain a public benefit. These circumstances justify broader access to information.

Overlap Between Law Enforcement and Oversight

Comment: Some commenters expressed concern that the NPRM's provisions permitting disclosures for health oversight and disclosures for law enforcement overlapped, and that the overlap could create confusion among covered entities, members of the public, and government agencies. The commenters identified particular factors that could lead to confusion, including that (1) the phrase ''criminal, civil, or administrative proceeding'' appeared in the definitions of both law enforcement

and oversight; (2) the examples of oversight agencies listed in the preamble included a number of organizations that also conduct law enforcement activities; (3) the NPRM addressed the issue of disclosures to investigate health care fraud in the law enforcement section (§ 164.510(f)(5)), yet health care fraud investigations are central to the mission of some health care oversight agencies; (4) the NPRM established more stringent rules for disclosure of protected health information pursuant to an administrative subpoena issued for law enforcement than for disclosure pursuant to an oversight agency's administrative subpoena; and (5) the preamble, but not the NPRM regulation text, indicated that agencies conducting both oversight and law enforcement activities would be subject to the oversight requirements when conducting oversight activities.

Some commenters said that covered entities would be confused by the overlap between law enforcement and oversight and that this concern would lead to litigation over which rules should apply when an entity engaged in more than one of the activities listed under the exceptions in proposed § 164.510. Other commenters believed that covered entities could manipulate the NPRM's ambiguities in their favor, claim that the more stringent law enforcement disclosure rules always should apply, and thereby delay investigations. A few comments suggested that the confusion could be clarified by making the regulation text consistent with the preamble, by stating that when agencies conducting both law enforcement and oversight seek protected health information as part of their oversight activities, the oversight rules would apply.

Response: We agree that the boundary between disclosures for health oversight and disclosures for law enforcement proposed in the NPRM could have been more clear. Because many investigations, particularly investigations involving public benefit programs, have both health oversight and law enforcement aspects to them, and because the same agencies often perform both functions, drawing any distinction between the two functions is necessarily difficult. For example, traditional law enforcement agencies, such as the Federal Bureau of Investigation, have a significant role in health oversight. At the same time, traditional health oversight agencies, such as federal Offices of Inspectors General, often participate in criminal investigations.

To clarify the boundary between law enforcement and oversight for purposes of complying with this rule, we add new language in the final rule, at § 164.512(d)(2). This section indicates that health oversight activities do not include an investigation or activity in which the individual is the subject of the investigation or activity and the investigation or activity does not arise out of and is not directly related to health care fraud. In this rule, we describe investigations involving suspected health care fraud as investigations related to: (1) The receipt of health care; (2) a claim for public benefits related to health; or (3) qualification for, or receipt of public benefits or services where a patient's health is integral to the claim for public benefits or services. In such cases, where the individual is the subject of the investigation and the investigation does not relate to health care fraud, identified as investigations regarding issues (a) through (c), the rules regarding disclosure for law enforcement purposes (see § 164.512(f)) apply.

Where the individual is not the subject of the activity or investigation, or where the investigation or activity relates to health care fraud, a covered entity may make a disclosure pursuant to § 164.512(d)(1), allowing uses and disclosures for health oversight activities. For example, when the U.S. Department of Labor's Pension and Welfare Benefits Administration (PWBA) needs to analyze protected health information about health plan enrollees in order to conduct an audit or investigation of the health plan (*i.e.,* the enrollees are not subjects of the investigation) to investigate potential fraud by the health plan, the health plan may disclose protected health information to the PWBA under the health oversight rules.

To clarify further that health oversight disclosure rules apply generally in health care fraud investigations (subject to the exception described above), in the final rule, we eliminate proposed § 164.510(f)(5)(i), which would have established requirements for disclosure related to health fraud for law enforcement purposes. All disclosures of protected health information that would have been permitted under proposed § 164.510(f)(5)(i) are permitted under § 164.512(d).

We also recognize that sections 201 and 202 of HIPAA, which established a federal Fraud and Abuse Control Program and the Medicare Integrity Program, identified health care fraud-fighting as a critical national priority. Accordingly, under the final rule, in joint law enforcement/oversight investigations involving suspected health care fraud, the health oversight disclosures apply, even if the individual also is the subject of the investigation.

We also recognize that in some cases, health oversight agencies may conduct joint investigations with other oversight agencies involved in investigating claims for benefits unrelated to health. For example, in some cases, a state Medicaid agency may be working with officials of the Food Stamps program to investigate suspected fraud involving Medicaid and Food Stamps. While this issue was not raised specifically in the comments, we add new language (§ 164.512(d)(3)) to provide guidance to covered entities in such situations. Specifically, we clarify that if a health oversight investigation is conducted in conjunction with an oversight activity related to a claim for benefits unrelated to health, the joint activity or investigation is considered health oversight for purposes of the rule, and the covered entities may disclose protected health information pursuant to the health oversight provisions.

Comment: An individual commenter recommended requiring authorization for disclosure of patient records in fraud investigations, unless the individual was the subject or target of the investigation. This commenter recommended requiring a search warrant for cases in which the individual was the subject and stating that fraud investigators should have access to the minimum necessary patient information.

Response: As described above, we recognize that in some cases, activities include elements of both law enforcement and health oversight. Because we consider both of these activities to be critical national priorities, we do not require covered entities to obtain authorization for disclosure of protected health information to law enforcement or health oversight agencies—including those oversight activities related to health care fraud. We believe that investigations involving health care fraud represent health oversight rather than law enforcement. Accordingly, as indicated above, we remove proposed § 164.510(f)(5)(i) from the law enforcement section of the proposed rule and clarify that all disclosures of protected health information for health oversight are permissible without authorization. As discussed in greater detail in § 164.514, the final rule's minimum necessary standard applies to disclosures under § 164.512 unless the disclosure is required by law under § 164.512(a).

Comment: A large number of commenters expressed concern about the potential for health oversight agencies to become, in effect, the ''back door'' for law enforcement access to such information. The commenters suggested that health oversight agencies could use their relatively unencumbered access to protected health information to circumvent the more stringent process requirements that otherwise would apply to disclosures for law enforcement purposes. These commenters urged us to prohibit health oversight agencies from re-disclosing protected health information to law enforcement.

Response: As indicated above, we do not intend for the rule's permissive approach to health oversight or the absence of specific documentation to permit the government to gather large amounts of protected health information for purposes unrelated to health oversight as defined in the rule, and we do not intend for these oversight provisions to serve as a ''back door'' for law enforcement access to protected health information. While we do not have the statutory authority to regulate law enforcement and oversight agencies' re-use and re-disclosure of protected health information, we strongly support enactment of comprehensive privacy legislation that would govern public agencies' re-use and re-disclosure of this information. Furthermore, in an effort to prevent health oversight provisions from becoming the back door to law enforcement access to protected health information, the President is issuing an Executive Order that places strict limitations on the use of protected health information gathered in the course of an oversight investigation for law enforcement activities.

Comment: One commenter asked us to allow the requesting agency to decide whether a particular request for protected health information was for law enforcement or oversight purposes.

Response: As described above, we clarify the overlap between law enforcement disclosures and health oversight disclosures based on the privacy and liberty interests of the individual (whether the individual also is the subject of the official inquiry) and the nature of the public interest (whether the inquiry relates to health care fraud or to another potential violation of law). We believe it is more appropriate to establish these criteria than to leave the decision to the discretion of an agency that has a stake in the outcome of the investigation.

Section 164.512(e)—Disclosures for Judicial and Administrative Proceedings

Comment: A few commenters suggested that the final rule not permit disclosures without an authorization for judicial and administrative proceedings.

Response: We disagree. Protected health information is necessary for a variety of reasons in judicial and administrative proceedings. Often it may be critical evidence that may or may not be about a party. Requiring an authorization for all such disclosures would severely impede the review of legal and administrative claims. Thus, we have tried to balance the need for the information with the individual's privacy. We believe the approach described above provides individuals with the opportunity to object to disclosures and provides a mechanism through which their privacy interests are taken into account.

Comment: A few commenters sought clarification about the interaction between permissible disclosures for judicial and administrative proceedings, law enforcement, and health oversight.

Response: In the final rule, we state that the provision permitting disclosures without an authorization for judicial and administrative proceedings does not supersede other provisions in § 164.512 that would otherwise permit or restrict the use or disclosure of protected health information. Additionally, in the descriptive preamble of § 164.512, we provide further explanation of how these provisions relate to one another.

Comments: Many commenters urged the Secretary to revise the rule to state that it does not preempt or supersede existing rules and statutes governing judicial proceedings, including rules of evidence, procedure, and discovery. One commenter asserted that dishonest health care providers and others should not be able to withhold their records by arguing that state subpoena and criminal discovery statutes compelling disclosure are preempted by the privacy regulation. Other commenters maintained that there is no need to replace providers' current practice, which typically requires either a signed authorization from the patient or a subpoena to release medical information.

Response: These comments are similar to many of the more general preemption comments we received. For a full discussion of the Secretary's response on preemption issues, see part 160—subpart B.

Comment: One commenter stated that the proposed rule creates a conflict with existing rules and statutes governing judicial proceedings, including rules of evidence and discovery. This commenter stated that the rule runs afoul of state judicial procedures for enforcement of subpoenas that require judicial involvement only when a party seeks to enforce a subpoena.

Response: We disagree with this comment. The final rule permits covered entities to disclose protected health information for any judicial or administrative procedure in response to a subpoena, discovery request, or other lawful process if the covered entity has received satisfactory assurances that the party seeking the disclosure has made reasonable efforts to ensure that the individual has been given notice of the request or has made reasonable efforts to secure a qualified protective order from a court or administrative tribunal. A covered entity may disclose protected health information in response to a subpoena, discovery request, or other lawful process without a satisfactory assurance if it has made reasonable efforts to provide the individual with such notice or to seek a qualified protected order itself. These rules do not require covered entities or parties seeking the disclosure of protected health information to involve the judiciary; they may choose the notification option rather than seeking a qualified protective order.

Many states have already enacted laws that incorporate these concepts. In California, for instance, an individual must be given ten days notice that his or her medical records are being subpoenaed from a health care provider and state law requires that the party seeking the records furnishes the health care provider with proof that the notice was given to the individual. In Montana, a party seeking discovery or compulsory process of medical records must give notice to the individual at least ten days in advance of serving the request on a health care provider, Service of the request must be accompanied by written certification that the procedure has been followed. In Rhode Island, an individual must be given notice that his or her medical records are being subpoenaed and notice of his or her right to object. The party serving the subpoena on the health care provider must provide written certification to the provider that: (1) This procedure has been followed, (2) twenty days have passed from the date of service, and (3) no challenge has been made to the disclosure or the court has ordered disclosure after resolution of a legal court challenge. In Washington, an individual must be given at least fourteen days from the date of service of notice that his or her health information is the subject of a

discovery request or compulsory process to obtain a protective order. The notice must identify the health care provider from whom the information is sought, specify the health care information that is sought, and the date by which a protective order must be obtained in order to prevent the provider from disclosing the information.

Comment: A few commenters expressed concern that the rule would place unnecessary additional burdens on health care providers because when they receive a request for disclosure in connection with an administrative or judicial procedure, they would have to determine whether the litigant's health was at issue before they made the disclosure. A number of commenters complained that this requirement would make it too easy for litigants to obtain protected health information. One commenter argued that litigants should not be able to circumvent state evidentiary rules that would otherwise govern disclosure of protected health information simply upon counsel's statement that the other party's medical condition or history is at issue.

Other commenters, however, urged that disclosure without authorization should be permitted whenever a patient places his or her medical condition or history at issue and recommended requiring the request for information to include a certification to this effect. Only if another party to litigation has raised a medical question, do these commenters believe a court order should be required. Similarly, one commenter supported a general requirement that disclosure without authorization be permitted only with a court order unless the patient has placed his or her physical or mental condition at issue.

Response: We agree with the concerns expressed by several commenters about this provision and have eliminated this requirement from the final rule.

Comment: A number of commenters stated that the proposed rule should be modified to permit disclosure without authorization pursuant to a lawful subpoena. One commenter argued that the provision would limit the scope of the Inspector General's subpoena power for judicial and administrative proceedings to information concerning a litigant whose health condition or history is at issue, and would impose a requirement that the Inspector General provide a written certification to that effect. Other commenters stated that the proposed rule would seriously impair the ability of state agencies to conduct administrative hearings on physician licensing and disciplinary matters. These commenters stated that current practice is to obtain information using subpoenas.

Other commenters argued that disclosure of protected health information for judicial and administrative proceedings should require a court order and/or judicial review unless the subject of the information consents to disclosure. These commenters believed that an attorney's certification should not be considered sufficient authority to override an individual's privacy, and that the proposed rule made it too easy for a party to litigation to obtain information about the other party.

Response: As a general matter, we agree with these comments. As noted, the final rule deletes the provision that would permit a covered entity to disclose protected health information pursuant to an attorney's certification that the individual is a party to the litigation and has put his or her medical condition at issue. Under the final rule, covered entities may disclose protected health information in response to a court or administrative order, provided that only the protected health information expressly authorized by the order is disclosed. Covered entities may also disclose protected health information in response to a subpoena, discovery request, or other lawful process without a court order, but only if the covered entity receives satisfactory assurances that the party seeking disclosure has made reasonable efforts to ensure that the individual has been notified of the request or that reasonable efforts have been made by the party seeking the information to secure a qualified protective order. Additionally, a covered entity may disclose protected health information in response to a subpoena, discovery request, or other lawful process without a satisfactory assurance if it makes reasonable efforts to provide the individual with such notice or to seek a qualified protected order itself.

We also note that the final rule specifically provides that nothing in Subchapter C should be construed to diminish the authority of any Inspector General, including authority provided in the Inspector General Act of 1978.

Comment: A number of commenters expressed concern that the proposed rule would not permit covered entities to introduce material evidence in proceedings in which, for example, the provisions of an insurance contract are at issue, or when a billing or payment issue is presented. They noted that although the litigant may be the owner of an insurance policy, he or she may not be the insured individual to whom the health information pertains. In addition, they stated that the medical condition or history of a deceased person may be at issue when the deceased person is not a party.

Response: We disagree. Under the final rule, a covered entity may disclose protected health information without an authorization pursuant to a court or administrative order. It may also disclose protected health information with an authorization for judicial or administrative proceedings in response to a subpoena, discovery request, or other lawful process without a court order, if the party seeking the disclosure provides the covered entity with satisfactory assurances that it has made reasonable efforts to ensure that the individual has been notified of the request or to seek a qualified protective order. Additionally, a covered entity may disclose protected health information in response to a subpoena, discovery request, or other lawful process without a satisfactory assurance if it makes reasonable efforts to provide the individual with such notice or to seek a qualified protected order itself. Therefore, a party may obtain the information even if the subject of the information is not a party to the litigation or deceased.

Comment: A few commenters argued that disclosure of protected health information should be limited only to those cases in which the individual has consented or a court order has been issued compelling disclosure.

Response: The Secretary believes that such an approach would impose an unreasonable burden on covered entities and the judicial system and that greater flexibility is necessary to assure that the judicial and administrative systems function smoothly. We understand that even those states that have enacted specific statutes to protect the privacy of health information have not imposed requirements as strict as these commenters would suggest.

Comment: Many commenters asked that the final rule require the notification of the disclosure be provided to the individual whose health information is subject to disclosure prior to the disclosure as part of a judicial or administrative proceeding. Most of these commenters also asked that the rule require that the individual who is the subject of a disclosure be given an opportunity to object to the disclosure. A few commenters suggested that patients be given ten days to object before requested information may be disclosed and recommend that the rule require the requester to provide a certification that notice has been provided and that ten days have passed

with no objection from the subject of the information. Some commenters suggested that if a subpoena for disclosure is not accompanied by a court order, the covered entities be prohibited from disclosing protected health information unless the individual has been given notice and an opportunity to object. Another commenter recommended requiring, in most circumstances, notice and an opportunity to object before a court order is issued and requiring the requestor of information to provide a signed document attesting the date of notification and forbid disclosure until ten days after notice is given.

Response: We agree that in some cases the provision of notice with an opportunity to object to the disclosure is appropriate. Thus, in the final rule we provide that a covered entity may disclose protected health information in response to a subpoena, discovery request or other lawful process that is not accompanied by a court order if it receives satisfactory assurance from the party seeking the request that the requesting party has made a good faith attempt to provide written notice to the individual that includes sufficient information about the litigation or proceeding to permit the individual to raise an objection to the court or administrative tribunal and that the time for the individual to raise objections has elapsed (and that none were filed or all have been resolved). Covered entities may make reasonable efforts to provide such notice as well.

In certain instances, however, the final rule permits covered entities to disclose protected health information for judicial and administrative proceedings without notice to the individual if the party seeking the request has made reasonable efforts to seek a qualified protective order, as described in the rule. A covered entity may also make reasonable efforts to seek a qualified protective order in order to make the disclosure. Additionally, a covered entity may disclose protected health information for judicial and administrative proceedings in response to an order of a court or administrative tribunal provided that the disclosure is limited to only that information that is expressly authorized by the order. The Secretary believes notice is not necessary in these instances because a court or administrative tribunal is in the best position to evaluate the merits of the arguments of the party seeking disclosure and the party who seeks to block it before it issues the order and that imposing further procedural obstacles before a covered entity may honor that disclosure request is unnecessary.

Comment: Many commenters urged the Secretary to require specific criteria for court and administrative orders. Many of these commenters proposed that a provision be added to the rule that would require court and administrative orders to safeguard the disclosure and use of protected health information. These commenters urged that the information sought must be relevant and material, as specific and narrowly drawn as reasonably practicable, and only disclosed if de-identified information could not reasonably be used.

Response: The Secretary's authority is limited to covered entities. Therefore, we do not impose requirements on courts and administrative tribunals. However, we note that the final rule limits the permitted disclosures by covered entities in court or administrative proceedings to only that information which is specified in the order from a court or an administrative body should provide a degree of protection for individuals from unnecessary disclosure.

Comment: Several commenters asked that the ''minimum necessary'' standard not apply to disclosures made pursuant to a court order because individuals could then use the rule to contest the scope of discovery requests. However, many other commenters recommended that the rule permit disclosure only of information ''reasonably necessary'' to respond to a subpoena. These commenters raised concerns with applying the ''minimum necessary'' standard in judicial and administrative proceedings, but did not believe the holder of protected health information should have blanket authority to disclose all protected health information. Some of the commenters urged that disclosure of any information about third parties that may be included in the medical records of another person— for example, the HIV status of a partner—be prohibited. Finally, some commenters disagreed with the proposed rule because it did not require covered entities to evaluate the validity of subpoenas and discovery requests to determine whether these requests ask for the ''minimum necessary'' or ''reasonably necessary'' amount of information.

Response: Under the final rule, if the disclosure is pursuant to an order of a court or administrative tribunal, covered entities may disclose only the protected health information expressly authorized by the order. In these instances, a covered entity is not required to make a determination whether or not the order might otherwise meet the minimum necessary requirement.

If the disclosure is pursuant to a satisfactory assurance from the party seeking the disclosure, at least a good faith attempt has been made to notify the individual in writing of the disclosure before it is made or the parties have sought a qualified protective order that prohibits them from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which the information was requested and that the information will be returned to the covered entity or destroyed at the end of the litigation or the proceeding. Alternatively, the covered entity may seek such notice or qualified protective order itself. This approach provides the individual with protections and places the burden on the parties to resolve their differences about the appropriateness and scope of disclosure as part of the judicial or administrative procedure itself before the order is issued, rather than requiring the covered entity to get involved in evaluating the merits of the dispute in order to determine whether or not the particular request is appropriate or too broad. In these cases, the covered entity must disclose only the protected health information that is the minimum amount necessary to achieve the purpose for which the information is sought.

We share the concern of the commenters that covered entities should redact any information about third parties before disclosing an individual's protected health information. During the fact-finding stage of our consideration of revisions to the proposed rule, we discussed this issue with representatives of covered entities. Currently, information about third parties is sometimes redacted by medical records personnel responding to requests for information. In particular, information regarding HIV status is treated with special sensitivity by these professionals. Although we considered including a special provision in the final rule prohibiting such disclosure, we decided that the revisions made to the proposed rule would provide sufficient protection. By restricting disclosure of protected health information to only that information specified in a court or administrative order or released pursuant to other types of lawful process only if the individual had notice and an opportunity to object or if the information was subject to a protective order, individuals who are concerned about disclosure of information concerning third parties will have the opportunity to raise that

issue prior to the request for disclosure being presented to the covered entity. We are reluctant to put the covered entity in the position of having to resolve disputes concerning the type of information that may be disclosed when that dispute should more appropriately be settled through the judicial or administrative procedure itself.

Comment: One commenter asked that the final regulation clarify that a court order is not required when disclosure would otherwise be permitted under the rule. This commenter noted that the preamble states that the requirement for a court order would not apply if the disclosure would otherwise be permitted under the rule. For example, disclosures of protected health information pursuant to administrative, civil, and criminal proceedings relating to ''health oversight'' are permitted, even if no court or administrative orders have been issued. However, the commenter was concerned that this principle only appeared in the preamble and not in the rule itself.

Response: Section 164.512(e)(4) of the final regulation contains this clarification.

Comment: One commenter was concerned that the rule is unclear as to whether governmental entities are given a special right to ''use'' protected health information that private parties do not have under the proposed regulation or whether governmental entities that seek or use protected health information are treated the same as private parties in their use of such information. This commenter urged that we clarify our intent regarding the use of protected health information by governmental entities.

Response: Generally governmental entities are treated the same as private entities under the rule. In a few clearly defined cases, a special rule applies. For instance, under § 164.504(e)(3), when a covered entity and its business associate are both governmental entities, they may enter into a memorandum of understanding or adopt a regulation with the force and effect of law that incorporates the requirements of a business associate contract, rather than having to negotiate a business associate contract itself.

Comment: One commenter recommended that final rule state that information developed as part of a quality improvement or medical error reduction program may not be disclosed under this provision. The commenter explained that peer review information developed to identify and correct systemic problems in delivery of care must be protected from disclosure to allow a full discussion of the root causes of such events so they may be identified and addressed. According to the commenter, this is consistent with peer review protections afforded this information by the states.

Response: The question of whether or not such information should be protected is currently the subject of debate in Congress and in the states. It would be premature for us to adopt a position on this issue until a clear consensus emerges. Under the final rule, no special protection against disclosure is provided for peer review information of the type the commenter describes. However, unless the request for disclosure fits within one of the categories of permitted or required disclosures under the regulation, it may not be disclosed. For instance, if disclosure of peer review information is required by another law (such as Medicare or a state law), covered entities subject to that law may disclose protected health information consistent with the law.

Comment: One commenter stated that the requirements of this section are in conflict with Medicare contractor current practices, as defined by the HCFA Office of General Counsel and suggested that the final rule include more specific guidelines.

Response: Because the commenter failed to indicate the nature of these conflicts, we are unable to respond.

Comment: One commenter stated that the rule should require rather than permit disclosure pursuant to court orders.

Response: Under the statutory framework adopted by Congress in HIPAA, a presumption is established that the data contained in an individual's medical record belongs to the individual and must be protected from disclosure to third parties. The only instance in which covered entities holding that information *must* disclose it is if the individual requests access to the information himself or herself. In the final rule (as in the proposed rule), covered entities *may* use or disclose protected health information under certain enumerated circumstances, but are not required to do so. We do not believe that this basic principle should be compromised merely because a court order has been issued. Consistent with this principle, we provide covered entities with the flexibility to deal with circumstances in which the covered entity may have valid reasons for declining to release the protected health information without violating this regulation.

Comment: One commenter noted that in some states, public health records are not subject to discovery, and that the proposed rule would not permit disclosure of protected health information pursuant to court order or subpoena if the disclosure is not allowed by state law. The commenter requested clarification as to whether a subpoena in a federal civil action would require disclosure if a state law prohibiting the release of public health records existed.

Response: As explained above, the final rule permits, but does not require, disclosure of protected health information pursuant to a court order. Under the applicable preemption provisions of HIPAA, state laws relating to the privacy of medical information that are more stringent than the federal rules are not preempted. To the extent that an applicable state law precludes disclosure of protected health information that would otherwise be permitted under the final rule, state law governs.

Comment: A number of commenters expressed concern that the proposed rule would negatively impact state and federal benefits programs, particularly social security and workers' compensation. One commenter requested that the final rule remove any possible ambiguity about application of the rule to the Social Security Administration's (SSA) evidence requests by permitting disclosure to all administrative level of benefit programs. In addition, several commenters stated that requiring SSA or states to provide the covered entity holding the protected health information with an individual's consent before it could disclose the information would create a huge administrative and paperwork burden with no added value to the individual. In addition, several other commenters indicated that states that make disability determinations for SSA also support special accommodation for SSA's determination process. They expressed concern that providers will narrowly interpret the HIPAA requirements, resulting in significant increases in processing time and program costs for obtaining medical evidence (especially purchased consultative examinations when evidence of record cannot be obtained). A few commenters were especially concerned about the impact on states and SSA if the final rule were to eliminate the NPRM's provision for a broad consent for ''all evidence from all sources.''

Some commenters also note that it would be inappropriate for a provider to make a minimum necessary determination in response to a request from SSA because the provider usually will not know the legal parameters of SSA's programs, or have access to the

individual's other sources of evidence. In addition, one commenter urged the Secretary to be sensitive to these concerns about delay and other negative impacts on the timely determination of disability by SSA for mentally impaired individuals.

Response: Under the final rule, covered entities may disclose protected health information pursuant to an administrative order so the flow of protected health information from covered entities to SSA and the states should not be disrupted.

Although some commenters urged that special rules should be included for state and federal agencies that need protected health information, the Secretary rejects that suggestion because, wherever possible, the public and the private sectors should operate under the same rules regarding the disclosure of health information. To the extent the activities of SSA constitute an actual administrative tribunal, covered entities must follow the requirements of § 164.512(e), if they wish to disclose protected health information to SSA in those circumstances. Not all administrative inquiries are administrative tribunals, however. If SSA's request for protected health information comes within another category of permissible exemptions, a covered entity, following the requirements of the applicable section, may disclose the information to SSA. For example, if SSA seeks information for purposes of health oversight, a covered entity that wishes to disclose the information to SSA may do so under § 164.512(d) and not § 164.512(e). If the disclosure does not come within one of the other permissible disclosures would a covered entity need to meet the requirements of § 164.512(e). If the SSA request does not come within another permissible disclosure, the agency will be treated like anyone else under the rules.

The Secretary recognizes that even under current circumstances, professional medical records personnel do not always respond unquestioningly to an agency's request for health information. During the fact finding process, professionals charged with managing provider response to requests for protected health information indicated to us that when an agency's request for protected health information is over broad, the medical records professional will contact the agency and negotiate a more limited request. In balancing the interests of individuals against the need of governmental entities to receive protected health information, we think that applying the minimum necessary standard is appropriate and that covered entities should be responsible for ensuring that they disclose only that protected health information that is necessary to achieve the purpose for which the information is sought.

Comment: In a similar vein, one commenter expressed concern that the proposed rule would adversely affect the informal administrative process usually followed in processing workers' compensation claims. Using formal discovery is not always possible, because some programs do not permit it. The commenter urged that the final rule must permit administrative agencies, employers, and workers' compensation carriers to use less formal means to obtain relevant medical evidence while the matter is pending before the agency. This commenter asked that the rule be revised to permit covered entities to disclose protected health information without authorization for purposes of federal or state benefits determinations at all levels of processing, from the initial application through continuing disability reviews.

Response: If the disclosure is required by a law relating to workers' compensation, a covered entity may disclose protected health information as authorized by and to the extent necessary to comply with that law under § 164.512(l). If the request for protected health information in connection with a workers' compensation claim is part of an administrative proceeding, a covered entity must meet the requirements set forth in § 164.512(e), and discussed above, before disclosing the information. As noted, one permissible manner by which a covered entity may disclose protected health information under § 164.512(e) is if the party seeking the disclosure makes reasonable efforts to provide notice to the individual as required by this provision. Under this method, the less formal process noted by the commenter would not be disturbed. Covered entity may disclose protected health information in response to other types of requests only as permitted by this regulation.

Section 164.512(f)—Disclosures for Law Enforcement Purposes

General Comments on Proposed § 164.510(f)

Comment: Some commenters argued that current law enforcement use of protected health information was legitimate and important. These commenters cited examples of investigations and prosecutions for which protected health information is needed, from white collar insurance fraud to violent assault, to provide incriminating evidence or to exonerate a suspect, to determine what charges are warranted and for bail decisions. For example, one commenter argued that disclosure of protected health information for law enforcement purposes should be exempt from the rule, because the proposed regulation would hamper Drug Enforcement Administration investigations. A few commenters argued that effective law enforcement requires early access to as much information as possible, to rule out suspects, assess severity of criminal acts, and for other purposes. A few commenters noted the difficulties criminal investigators and prosecutors face when fighting complex criminal schemes. In general, these commenters argued that all disclosures of protected health information to law enforcement should be allowed, or for elimination of the process requirements proposed in § 164.510(f)(1).

Response: The importance and legitimacy of law enforcement activities are beyond question, and they are not at issue in this regulation. We permit disclosure of protected health information to law enforcement officials without authorization in some situations precisely because of the importance of these activities to public safety. At the same time, individuals' privacy interests also are important and legitimate. As with all the other disclosures of protected health information permitted under this regulation, the rules we impose attempt to balance competing and legitimate interests.

Comment: Law enforcement representatives stated that law enforcement agencies had a good track record of protecting patient privacy and that additional restrictions on their access and use of information were not warranted. Some commenters argued that no new limitations on law enforcement access to protected health information were necessary, because sufficient safeguards exist in state and federal laws to prevent inappropriate disclosure of protected health information by law enforcement.

Response: Disclosure of protected health information by law enforcement is not at issue in this regulation. Law enforcement access to protected health information in the first instance, absent any re-disclosure by law enforcement, impinges on individuals' privacy interests and must therefore be justified by a public purpose that outweighs individuals' privacy interests.

We do not agree that sufficient safeguards already exist in this area. We are not aware of, and the comments did

not provide, evidence of a minimum set of protections for individuals relating to access by law enforcement to their protected health information. Federal and state laws in this area vary considerably, as they do for other areas addressed in this final rule. The need for standards in this area is no less critical than in the other areas addressed by this rule.

Comment: Many commenters argued that no disclosures of protected health information should be made to law enforcement (absent authorization) without a warrant issued by a judicial officer after a finding of probable cause. Others argued that a warrant or subpoena should be required prior to disclosure of protected health information unless the disclosure is for the purposes of identifying a suspect, fugitive, material witness, or missing persons, as described in proposed § 164.510(f)(2). Some commenters argued that judicial review prior to release of protected health information to law enforcement should be required absent the exigent and urgent circumstances identified in the NPRM in § 164.510(f)(3) and (5), or absent ''a compelling need'' or similar circumstances.

Response: In the final rule, we attempt to match the level of procedural protection for privacy required by this rule with the nature of the law enforcement need for access, the existence of other procedural protections, and individuals' privacy interests. Where other rules already impose procedural protections, this rule generally relies on those protections rather than imposing new ones. Thus, where access to protected health information is granted after review by an independent judicial officer (such as a court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer), no further requirements are necessary. Similarly, because information disclosed to a grand jury is vital to law enforcement purposes and is covered by secrecy protection, this rule allows disclosure with no further process.

We set somewhat stricter standards for disclosure of protected health information pursuant to administrative process, such as administrative subpoenas, summonses, and civil or authorized investigative demands. In these cases, the level of existing procedural protections is lower than for judicially-approved or grand jury disclosures. We therefore require a greater showing, specifically, the three-part test described in § 164.512(f)(1)(ii), before the covered entity is permitted to release protected health information. Where the information to be disclosed is about the victim of a crime, privacy interests are heightened and we require the victim's agreement prior to disclosure in most instances.

In the limited circumstances where law enforcement interests are heightened, we allow disclosure of protected health information without prior legal process or agreement, but we impose procedural protections such as limits on the information that may lawfully be disclosed, limits on the circumstances in which the information may be disclosed, and requirements for verifying the identity and authority of the person requesting the disclosures. For example, in some cases law enforcement officials may seek limited but focused information needed to obtain a warrant. A witness to a shooting may know the time of the incident and the fact that the perpetrator was shot in the left arm, but not the identity of the perpetrator. Law enforcement would then have a legitimate need to ask local emergency rooms whether anyone had presented with a bullet wound to the left arm near the time of the incident. Law enforcement may not have sufficient information to obtain a warrant, but instead would be seeking such information. In such cases, when only limited identifying information is disclosed and the purpose is solely to ascertain the identity of a person, the invasion of privacy would be outweighed by the public interest. For such circumstances, we allow disclosure of protected health information in response to a law enforcement inquiry where law enforcement is seeking to identify a suspect, fugitive, material witness, or missing person, but allow only disclosure of a limited list of information.

Similarly, it is in the public interest to allow covered entities to take appropriate steps to protect the integrity and safety of their operations. Therefore, we permit covered entities on their own initiative to disclose to law enforcement officials protected health information for this purpose. However, we limit such disclosures to protected health information that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity.

We shape the rule's provisions with respect to law enforcement according to the limited scope of our regulatory authority under HIPAA, which applies only to the covered entities and not to law enforcement officials. We believe the rule sets the correct standards for when an exception to the rule of non-disclosure is appropriate for law enforcement purposes. There may be advantages, however, to legislation that applies the appropriate standards directly to judicial officers, prosecutors in grand juries, and to those making administrative or other requests for protected health information, rather than to covered entities. These advantages could include measures to hold officials accountable if they seek or receive protected health information contrary to the legal standard. In Congressional consideration of law enforcement access, there have also been useful discussions of other topics, such as limits on re-use of protected health information gathered in the course of health oversight activities. The limitations on our regulatory authority provide additional reason to support comprehensive medical privacy legislation.

Comment: A few commenters cited existing sanctions for law enforcement officials who violate the rights of individuals in obtaining evidence, ranging from suppression of that evidence to monetary penalties, and argued that such sanctions are sufficient to protect patients' privacy interests.

Response: After-the-fact sanctions are important, but they are effective only when coupled with laws that establish the ground rules for appropriate behavior. That is, a sanction applies only where some other rule has been violated. This regulation sets such basic ground rules. Further, under the HIPAA statutory authority, we cannot impose sanctions on law enforcement officials or require suppression of evidence. We must therefore rely on rules that regulate disclosure of protected health information by covered entities in the first instance.

Comment: Several commenters argued that disclosure of protected health information under § 164.510(f) should be mandatory, not just permitted. Others argued that we should mandate disclosure of protected health information in response to Inspector General subpoenas. A few commenters argued that we should require all covered entities to include disclosure of protected health information to law enforcement in their required notice of privacy practices.

Response: The purpose of this regulation is to protect individuals' privacy interests, consistent with other important public activities. Other laws set the rules governing those public activities, including when health information is necessary for their effective operation. See discussion of § 164.512(a).

Comment: Some commenters questioned whether the Secretary had statutory authority to directly or indirectly impose new procedural or substantive requirements on otherwise lawful legal process issued under existing federal and state rules. They argued that, while the provisions are imposed on ''covered entities,'' the rule would result in law enforcement officials being compelled to modify current practices to harmonize them with the requirements this rule imposes on covered entities. A number of state law enforcement agencies argued that the rule would place new burdens on state administrative subpoenas and requests that are intrusive in state functions. At least one commenter argued that the requirement for prior process places unreasonable restrictions on the right of the states to regulate law enforcement activities.

Response: This rule regulates the ability of health care clearinghouses, health plans, and covered health care providers to use and disclose health information. It does not regulate the behavior of law enforcement officials or the courts, nor does it prevent states from regulating law enforcement officials. All regulations have some effects on entities that are not directly regulated. We have considered those effects in this instance and have determined that the provisions of the rule are necessary to protect the privacy of individuals.

Comment: One commenter argued that state licensing boards should be exempt from restrictions placed on law enforcement officials, because state licensing and law enforcement are different activities.

Response: Each state's law determines what authorities are granted to state licensing boards. Because state laws differ in this regard, we cannot make a blanket determination that state licensing officials are or are not law enforcement officials under this regulation. We note, however, that the oversight of licensed providers generally is included as a health oversight activity at § 164.512(d).

Relationship to Existing Rules and Practices

Comment: Many commenters expressed concern that the proposed rule would have expanded current law enforcement access to protected health information. Many commenters said that the NPRM would have weakened their current privacy practices with respect to law enforcement access to health records. For example, some of the commenters arguing that a warrant or subpoena should be required prior to disclosure of protected health information unless the disclosure is for the purposes of identifying a suspect, fugitive, material witness, or missing persons, did so because they believed that such a rule would be consistent with current state law practices.

Response: This regulation does not expand current law enforcement access to protected health information. We do not mandate any disclosures of protected health information to law enforcement officials, nor do we make lawful any disclosures of protected health information which are unlawful under other rules and regulations. Similarly, this regulation does not describe a set of ''best practices.'' Nothing in this regulation should cause a covered entity to change practices that are more protective of privacy than the floor of protections provided in this regulation.

This regulation sets forth the minimum practices which a covered entity must undertake in order to avoid sanctions under the HIPAA. We expect and encourage covered entities to exercise their judgment and professional ethics in using and disclosing health information, and to continue any current practices that provide privacy protections greater than those mandated in this regulation.

Comment: Many commenters asserted that, today, consent or judicial review always is required prior to release of protected health information to law enforcement; therefore, they said that the proposed rule would have lessened existing privacy protections.

Response: In many situations today, law enforcement officials lawfully obtain health information absent any prior legal process and absent exigent circumstances. The comments we received on the NPRM, both from law enforcement and consumer advocacy groups, describe many such situations. Moreover, this rule sets forth minimum privacy protections and does not preempt more stringent, pre-existing standards.

Comment: Some commenters argued that health records should be entitled to at least as much protection as cable subscription records and video rental records.

Response: We agree. The Secretary, in presenting her initial recommendations on the protection of health information to the Congress in 1997, stated that, ''When Congress looked at the privacy threats to our credit records, our video records, and our motor vehicle records, it acted quickly to protect them. It is time to do the same with our health care records' (Testimony of Donna E. Shalala, Secretary, U. S. Department of Health and Human Services, before the Senate Committee on Labor & Human Resources, September 11, 1997). However, the limited jurisdiction conferred on us by the HIPAA does not allow us to impose such restrictions on law enforcement officials or the courts.

Comment: At least one commenter argued that the regulation should allow current routine uses for law enforcement under the Privacy Act.

Response: This issue is discussed in the ''Relationship to Other Federal Laws'' preamble discussion of the Privacy Act.

Comment: A few commenters expressed concern that people will 8be less likely to provide protected health information for public health purposes if they fear the information could be used for law enforcement purposes.

Response: This regulation does not affect law enforcement access to records held by public health authorities, nor does it expand current law enforcement access to records held by covered entities. These agencies are for the most part not covered entities under HIPAA. Therefore, this regulation should not reduce current cooperation with public health efforts.

Relationship to Other Provisions of This Regulation

Comment: Several commenters pointed out an unintended interaction between proposed §§ 164.510(f) and 164.510(n). Because proposed § 164.510(n), allowing disclosures mandated by other laws, applied only if the disclosure would not fall into one of the categories of disclosures provided for in § 164.510 (b)–(m), disclosures of protected health information mandated for law enforcement purposes by other law would have been preempted.

Response: We agree, and in the final rule we address this unintended interaction. It is not our intent to preempt these laws. To clarify the interaction between these provisions, in the final rule we have specifically added language to the paragraph addressing disclosures for law enforcement that permits covered entities to comply with legal mandates, and have included a specific cross reference in the provision of the final rule that permits covered entities to make other disclosures required by law. See § 164.512(a).

Comment: Several commenters argued that, when a victim of abuse or of a crime has requested restrictions on disclosure, the restrictions should be communicated to any law enforcement officials who receive that protected health information.

Response: We do not have the authority to regulate law enforcement

use and disclosure of protected health information, and therefore we could not enforce any such restrictions communicated to law enforcement officials. For this reason, we determined that the benefits to be gained from requiring communication of restrictions would not outweigh the burdens such a requirement would place on covered entities. We expect that professional ethics will guide health care providers' communications to law enforcement officials about the welfare of victims of abuse or other crime.

Comment: Some commenters argued against imposing the ''minimum necessary'' requirement on disclosure of protected health information to law enforcement officials. Some law enforcement commenters expressed concern that the ''minimum necessary'' test could be ''manipulated'' by a covered entity that wished to withhold relevant evidence. A number of covered entities complained that they were ill-equipped to substitute their judgment for that of law enforcement for what was the minimum amount necessary, and they also argued that the burden of determining the ''minimum necessary'information should be transferred to law enforcement agencies. Some commenters argued that imposing such ''uninformed'' discretion on covered entities would delay or thwart legitimate investigations, and would result in withholding information that might exculpate an individual or might be necessary to present a defendant's case. One comment suggested that covered entities have ''immunity'' for providing too much information to law enforcement.

Response: The ''minimum necessary'' standard is discussed at § 164.514.

Comment: A few commenters asked us to clarify when a disclosure is for a ''Judicial or Administrative Proceeding'' and when it is for ''Law Enforcement'' purposes.

Response: In the final rule we have clarified that § 164.512(e) relating to disclosures for judicial or administrative proceedings does not supersede the authority of a covered entity to make disclosures under other provisions of the rule.

Use of Protected Health Information After Disclosure to Law Enforcement

Comment: Many commenters recommended that we restrict law enforcement officials' re-use and re-disclosure of protected health information. Some commenters asked us to impose such restrictions, while other commenters noted that the need for such restrictions underscores the need for legislation. Another argued for judicial review prior to release of protected health information to law enforcement because this regulation cannot limit further uses or disclosures of protected health information once it is in the hands of law enforcement agencies.

Response: We agree that there are advantages to legislation that imposes appropriate restrictions directly on the re-use and re-disclosure of protected health information by many persons who may lawfully receive protected health information under this regulation, but whom we cannot regulate under the HIPAA legislative authority, including law enforcement agencies.

Comment: A few commenters expressed concern that protected health information about persons who are not suspects may be used in court and thereby become public knowledge. These commenters urged us to take steps to minimize or prevent such protected health information from becoming part of the public record.

Response: We agree that individuals should be protected from unnecessary public disclosure of health information about them. However, we do not have the statutory authority in this regulation to require courts to impose protective orders. To the extent possible within the HIPAA statutory authority, we address this problem in § 164.512(e), Judicial and Administrative Proceedings.

Comment: Some commenters argued that evidence obtained in violation of the regulation should be inadmissible at trial.

Response: In this regulation, we do not have the authority to regulate the courts. We can neither require nor prohibit courts from excluding evidence obtain in violation of this regulation.

Comments Regarding Proposed § 164.510(f)(1), Disclosures to Law Enforcement Pursuant to Process

Comments Supporting or Opposing a Requirement of Consent or Court Order

Comment: Some commenters argued that a rule that required a court order for every instance that law enforcement sought protected health information would impose substantial financial and administrative burdens on federal and state law enforcement and courts. Other commenters argued that imposing a new requirement of prior judicial process would compromise the time-sensitive nature of many investigations.

Response: We do not impose such a requirement in this regulation.

Comment: Many commenters argued that proposed § 164.510(f)(1) would have given law enforcement officials the choice of obtaining records with or without a court order, and that law enforcement ''will choose the least restrictive means of obtaining records, those that do not require review by a judge or a prosecutor.'' Several commenters argued that this provision would have provided the illusion of barriers—but no real barriers—to law enforcement access to protected health information. A few argued that this provision would have allowed law enforcement to regulate itself.

Response: We agree with commenters that, in some cases, a law enforcement official may have discretion to seek health information under more than one legal avenue. Allowing a choice in these circumstances does not mean an absence of real limits. Where law enforcement officials choose to obtain protected health information through administrative process, they must meet the three-part test required by this regulation.

Comment: At least one commenter argued for judicial review prior to disclosure of health information because the rule will become the ''de facto'' standard for release of protected health information.

Response: We do not intend for this regulation to become the ''de facto'' standard for release of protected health information. Nothing in this regulation limits the ability of states and other governmental authorities to impose stricter requirements on law enforcement access to protected health information. Similarly, we do not limit the ability of covered entities to adopt stricter policies for disclosure of protected health information not mandated by other laws.

Comment: A few commenters expressed concern that proposed § 164.510(f)(1) would have overburdened the judicial system.

Response: The comments did not provide any factual basis for evaluating this concern.

Comment: Some commenters argued that, while a court order should be required, the standard of proof should be something other than ''probable cause.'' For example, one commenter argued that the court should apply the three-part test proposed in § 164.510(f)(1)(i)(C). Another commenter suggested a three-part test: The information is necessary, the need cannot be met with non-identifiable information, and the need of law enforcement outweighs the privacy interest of the patient. Some commenters suggested that we impose a ''clear and convincing'' standard. Another suggested that we require clear and convincing evidence that: (1) The

information sought is relevant and material to a legitimate criminal investigation; (2) the request is as specific and narrow as is reasonably practicable; (3) de-identified information, for example coded records, could not reasonably be used; (4) on balance, the need for the information outweighs the potential harm to the individuals and to patient care generally; and (5) safeguards appropriate to the situation have been considered and imposed. This comment also suggested the following as such appropriate safeguard: granting only the right to inspect and take notes; allowing copying of only certain portions of records; prohibiting removing records from the premises; placing limits on subsequent use and disclosure; and requiring return or destruction of the information at the earliest possible time.) Others said the court order should impose a ''minimum necessary'' standard.

Response: We have not revised the regulation in response to comments suggesting that we impose additional standards relating to disclosures to comply with court orders. Unlike administrative subpoenas, where there is no independent review of the order, court orders are issued by an independent judicial officer, and we believe that covered entities should be permitted under this rule to comply with them. Court orders are issued in a wide variety of cases, and we do not know what hardships might arise by imposing standards that would require judicial officers to make specific findings related to privacy.

Comment: At least one commenter argued that the proposed rule would have placed too much burden on covered entities to evaluate whether to release information in response to a court order. This comment suggested that the regulation allow disclosure to attorneys for assessment of what the covered entity should release in response to a court order.

Response: This regulation does not change current requirements on or rights of covered entities with respect to court orders for the release of health information. Where such disclosures are required today, they continue to be required under this rule. Where other law allows a covered entity to challenge a court order today, this rule will not reduce the ability of a covered entity to mount such a challenge. Under § 164.514, a covered entity will be permitted to rely on the face of a court order to meet this rule's requirements for verification of the legal authority of the request for information. A covered entity may disclose protected health information to its attorneys as needed, to perform health care operations, including to assess the covered entity's appropriate response to court orders. See definition of ''health care operations'' under § 164.501.

Comment: Many commenters argued that the regulation should prohibit disclosures of protected health information to law enforcement absent patient consent.

Response: We disagree with the comment. Requiring consent prior to any release of protected health information to a law enforcement official would unduly jeopardize public safety. Law enforcement officials need protected health information for their investigations in a variety of circumstances. The medical condition of a defendant could be relevant to whether a crime was committed, or to the seriousness of a crime. The medical condition of a witness could be relevant to the reliability of that witness. Health information may be needed from emergency rooms to locate a fleeing prison escapee or criminal suspect who was injured and is believed to have stopped to seek medical care.

These and other uses of medical information are in the public interest. Requiring the authorization of the subject prior to disclosure could make apprehension or conviction of some criminals difficult or impossible. In many instances, it would not be possible to obtain such consent, for example because the subject of the information could not be located in time (or at all). In other instances, the covered entity may not wish to undertake the burden of obtaining the consent. Rather than an across-the-board consent requirement, to protect individuals' privacy interests while also promoting public safety, we impose a set of procedural safeguards (described in more detail elsewhere in this regulation) that covered entities must ensure are met before disclosing protected health information to law enforcement officials.

In most instances, such procedural safeguards consist of some prior legal process, such as a warrant, grand jury subpoena, or an administrative subpoena that meets a three-part test for protecting privacy interests. When the information to be disclosed is about the victim of a crime, privacy interests are heightened and we require the victim's agreement prior to disclosure in most instances. In the limited circumstances where law enforcement interests are heightened and we allow disclosure of protected health information without prior legal process or agreement, the procedural protections include limits on the information that may lawfully be disclosed, the circumstances in which the information may be disclosed, and requirements for verifying the identity and authority of the person requesting the disclosures.

We also allow disclosure of protected health information to law enforcement officials without consent when other law mandates the disclosures. When such other law exists, another public entity has made the determination that law enforcement interests outweigh the individual's privacy interests in the situations described in that other law, and we do not upset that determination in this regulation.

Comment: Several commenters recommended requiring that individuals receive notice and opportunity to contest the validity of legal process under which their protected health information will be disclosed, prior to disclosure of their records to law enforcement. Some of these commenters recommended adding this requirement to provisions proposed in the NPRM, while others recommended establishing this requirement as part of a new requirement for a judicial warrant prior to all disclosures of protected health information to law enforcement. At least one of these commenters proposed an exception to such a notice requirement where notice might lead to destruction of the records.

Response: Above we discuss the reasons why we believe it is inappropriate to require consent or a judicial order prior to any release of protected health information to law enforcement. Many of those reasons apply here, and they lead us not to impose such a notice requirement.

Comment: A few commenters believed that the proposed requirements in § 164.510(f)(1) would hinder investigations under the Civil Rights for Institutionalized Persons Act (CRIPA).

Response: We did not intend that provision to apply to investigations under CRIPA, and we clarify in the final rule that covered entities may disclose protected health information for such investigations under the health oversight provisions of this regulation (see § 164.512(d) for further detail).

Comments Suggesting Changes to the Proposed Three-Part Test

Comment: Many commenters argued for changes to the proposed three-part test that would make the test more difficult to meet. Many of these urged greater, but unspecified, restrictions. Others argued that the proposed test was too stringent, and that it would have hampered criminal investigations and prosecutions. Some argued that it

was too difficult for law enforcement to be specific at the beginning of an investigation. Some argued that there was no need to change current practices, and they asked for elimination of the three-part test because it was ''more stringent'' than current practices and would make protected health information more difficult to obtain for law enforcement purposes. These commenters urged elimination of the three-part test so that administrative bodies could continue current practices without additional restrictions. Some of these argued for elimination of the three-part test for all administrative subpoenas; others argued for elimination of the three-part test for administrative subpoenas from various Inspectors General offices. A few commenters argued that the provisions in proposed § 164.510(f)(1) should be eliminated because they would have burdened criminal investigations and prosecutions but would have served ''no useful public purpose.''

Response: We designed the proposed three-part test to require proof that the government's interest in the health information was sufficiently important and sufficiently focused to overcome the individual's privacy interest. If the test were weakened or eliminated, the individual's privacy interest would be insufficiently protected. At the same time, if the test were significantly more difficult to meet, law enforcement's ability to protect the public interest could be unduly compromised.

Comment: At least one comment argued that, in the absence of a judicial order, protected health information should be released only pursuant to specific statutory authority.

Response: It is impossible to predict all the facts and circumstances, for today and into the future, in which law enforcement's interest in health information outweigh individuals' privacy interests. Recognizing this, states and other governments have not acted to list all the instances in which health information should be available to law enforcement officials. Rather, they specify some such instances, and rely on statutory, constitutional, and other limitations to place boundaries on the activities of law enforcement officials. Since the statutory authority to which the commenter refers does not often exist, many uses of protected health information that are in the public interest (described above in more detail) would not be possible under such an approach.

Comment: At least one commenter, an administrative agency, expressed concern that the proposed rule would have required its subpoenas to be approved by a judicial officer.

Response: This rule does not require judicial approval of administrative subpoenas. Administrative agencies can avoid the need for judicial review under this regulation by issuing subpoenas for protected health information only where the three-part test has been met.

Comment: Some commenters suggested alternative requirements for law enforcement access to protected health information. A few suggested replacing the three-part test with a requirement that the request for protected health information from law enforcement be in writing and signed by a supervisory official, and/or that the request ''provide enough information about their needs to allow application of the minimum purpose rule.''

Response: A rule requiring only that the request for information be in writing and signed fails to impose appropriate substantive standards for release of health information. A rule requiring only sufficient information for the covered entity to make a ''minimum necessary'' determination would leave these decisions entirely to covered entities' discretion. We believe that protection of individuals' privacy interests must start with a minimum floor of protections applicable to all. We believe that while covered entities may be free to provide additional protections (within the limits of the law), they should not have the ability to allow unjustified access to health information.

Comment: Some commenters argued that the requirement for an unspecified ''finding'' for a court order should be removed from the proposed rule, because it would have been confusing and would have provided no guidance to a court as to what finding would be sufficient.

Response: We agree that the requirement would have been confusing, and we delete this language from the final regulation.

Comment: A few commenters argued that the proposed three-part test should not be applied where existing federal or state law established a standard for issuing administrative process.

Response: It is the content of such a standard, not its mere existence, that determines whether the standard strikes an appropriate balance between individuals' privacy interests and the public interest in effective law enforcement activities. We assume that current authorities to issue administrative subpoena are all subject to some standards. When an existing standard provides at least as much protection as the three-part test imposed by this regulation, the existing standard is not disturbed by this rule. When, however, an existing standard for issuing administrative process provides less protection, this rule imposes new requirements.

Comment: Some covered entities said that they should not have been asked to determine whether the proposed three-part test has been met. Some argued that they were ill-equipped to make a judgment on whether an administrative subpoena actually met the three-part test, or that it was unfair to place the burden of making such determinations on covered entities. Some argued that the burden should have been on law enforcement, and that it was inappropriate to shift the burden to covered entities. Other commenters argued that the proposal would have given too much discretion to the record holders to withhold evidence without having sufficient expertise or information on which to make such judgments. At least one comment said that this aspect of the proposal would have caused delay and expense in the detection and prevention of health care fraud. The commenter believed that this delay and expense could be prevented by shifting to law enforcement and health care oversight the responsibility to determine whether standards have been met.

At least one commenter recommended eliminating the three-part test for disclosures of protected health information by small providers.

Some commenters argued that allowing covered entities to rely on law enforcement representation that the three-part test has been met would render the test meaningless.

Response: Because the statute does not bring law enforcement officials within the scope of this regulation, the rule must rely on covered entities to implement standards that protect individuals' privacy interests, including the three-part test for disclosure pursuant to administrative subpoenas. To reduce the burden on covered entities, we do not require a covered entity to second-guess representations by law enforcement officials that the three part test has been met. Rather, we allow covered entities to disclose protected health information to law enforcement when the subpoena or other administrative request indicates on its face that the three-part test has been met, or where a separate document so indicates. Because we allow such reliance, we do not believe that it is necessary or appropriate to reduce privacy protections for individuals who obtain care from small health care providers.

Comment: Some commenters ask for modification of the three-part test to include a balancing of the interests of law enforcement and the privacy of the individual, pointing to such provisions in the Leahy-Kennedy bill.

Response: We agree with the comment that the balancing of these interests is important in this circumstance. We designed the regulation's three-part test to accomplish that result.

Comment: At least one commenter recommended that ''relevant and material'' be changed to ''relevant,'' because ''relevant'' is a term at the core of civil discovery rules and is thus well understood, and because it would be difficult to determine whether information is ''material'' prior to seeing the documents. As an alternative, this commenter suggested explaining what we meant by ''material.''

Response: Like the term ''relevant,'' the term ''material'' is commonly used in legal standards and well understood.

Comment: At least one commenter suggested deleting the phrase ''reasonably practical'' from the second prong of the test, because, the commenter believed, it was not clear who would decide what is ''reasonably practical'' if the law enforcement agency and covered entity disagreed.

Response: We allow covered entities to rely on a representation on the face of the subpoena that the three-part test, including the ''reasonably practical'' criteria, is met. If a covered entity believes that a subpoena is not valid, it may challenge that subpoena in court just as it may challenge any subpoena that today it believes is not lawfully issued. This is true regardless of the specific test that a subpoena must meet, and is not a function of the ''reasonably practical'' criteria.

Comment: Some commenters requested elimination of the third prong of the test. One of these commenters suggested that the regulation should specify when de-identified information could not be used. Another recommended deleting the phrase ''could not reasonably be used'' from the third prong of the test, because the commenter believed it was not clear who would determine whether de-identified information ''could reasonably be used'' if the law enforcement agency and covered entity disagreed.

Response: We cannot anticipate in regulation all the facts and circumstances surrounding every law enforcement activity today, or in the future as technologies change. Such a rigid approach could not account for the variety of situations faced by covered entities and law enforcement officials, and would become obsolete over time. Thus, we believe it would not be appropriate to specify when de-identified information can or cannot be used to meet legitimate law enforcement needs.

In the final rule, we allow the covered entity to rely on a representation on the face of the subpoena (or similar document) that the three-part test, including the ''could not reasonably be used'' criteria, is met. If a covered entity believes that a subpoena is not valid, it may challenge that subpoena in court just as it may challenge today any subpoena that it believes is not lawfully issued. This is true regardless of the specific test that a subpoena must meet, and it is not a function of the ''could not reasonably be used'' criteria.

Comments Regarding Proposed § 164.510(f)(2), Limited Information for Identifying Purposes

Comment: A number of commenters recommended deletion of this provision. These commenters argued that the legal process requirements in proposed § 164.510(f)(1) should apply when protected health information is disclosed for identification purposes. At least one privacy group recommended that if the provision were not eliminated in its entirety, ''suspects'' should be removed from the list of individuals whose protected health information may be disclosed for identifying purposes. Many commenters expressed concern that this provision would allow compilation of large data bases of health information that could be use for purposes beyond those specified in this provision.

Response: We retain this provision in the final rule. We continue to believe that identifying fugitives, material witnesses, missing persons, and suspects is an important national priority and that allowing disclosure of limited identifying information for this purpose is in the public interest. Eliminating this provision—or eliminating suspects from the list of types of individuals about whom disclosure of protected health information to law enforcement is allowed—would impede law enforcement agencies'' ability to apprehend fugitives and suspects and to identify material witnesses and missing persons. As a result, criminals could remain at large for longer periods of time, thereby posing a threat to public safety, and missing persons could be more difficult to locate and thus endangered.

However, as described above and in the following paragraphs, we make significant changes to this provision, to narrow the information that may be disclosed and make clear the limited purpose of the provision. For example, the proposed rule did not state explicitly whether covered entities would have been allowed to initiate—in the absence of a request from law enforcement—disclosure of protected health information to law enforcement officials for the purpose of identifying a suspect, fugitive, material witness or missing person. In the final rule, we clarify that covered entities may disclose protected health information for identifying purposes only in response to a request by a law enforcement official or agency. A ''request by a law enforcement official or agency'' is not limited to direct requests, but also includes oral or written requests by individuals acting on behalf of a law enforcement agency, such as a media organization broadcasting a request for the public's assistance in identifying a suspect on the evening news. It includes ''Wanted'' posters, public announcements, and similar requests to the general public for assistance in locating suspects or fugitives.

Comment: A few commenters recommended additional restrictions on disclosure of protected health information for identification purposes. For example, one commenter recommended that the provision should either (1) require that the information to be disclosed for identifying purposes be relevant and material to a legitimate law enforcement inquiry and that the request be as specific and narrowly drawn as possible; or (2) limit disclosures to circumstances in which (a) a crime of violence has occurred and the perpetrator is at large, (b) the perpetrator received an injury during the commission of the crime, (c) the inquiry states with specificity the type of injury received and the time period during which treatment would have been provided, and (d) ''probable cause'' exists to believe the perpetrator received treatment from the provider.

Response: We do not agree that these additional restrictions are appropriate for disclosures of limited identifying information for purposes of locating or identifying suspects, fugitives, material witnesses or missing persons. The purpose of this provision is to permit law enforcement to obtain limited time-sensitive information without the process requirements applicable to disclosures for other purposes. Only limited information may be disclosed under this provision, and disclosure is permitted only in limited circumstances. We believe that these

safeguards are sufficient, and that creating additional restrictions would undermine the purpose of the provision and that it would hinder law enforcement's ability to obtain essential, time-sensitive information.

Comment: A number of law enforcement agencies recommended that the provision in the proposed rule be broadened to permit disclosure to law enforcement officials for the purpose of ''locating'' as well as ''identifying'' a suspect, fugitive, material witness or missing person.

Response: We agree with the comment and have changed the provision in the final rule. We believe that locating suspects, fugitives, material witnesses and missing persons is an important public policy priority, and that it can be critical to identifying these individuals. Further, efforts to locate suspects, fugitives, material witnesses, and missing persons can be at least as time-sensitive as identifying such individuals.

Comment: Several law enforcement agencies requested that the provision be broadened to permit disclosure of additional pieces of identifying information, such as ABO blood type and Rh factor, DNA information, dental records, fingerprints, and/or body fluid and tissue typing, samples and analysis. These commenters stated that additional identifying information may be necessary to permit identification of suspects, fugitives, material witnesses or missing persons. On the other hand, privacy and consumer advocates, as well as many individuals, were concerned that this section would allow all computerized medical records to be stored in a large law enforcement data base that could be scanned for matches of blood, DNA, or other individually identifiable information.

Response: The final rule seeks to strike a balance in protecting privacy and facilitating legitimate law enforcement inquiries. Specifically, we have broadened the NPRM's list of data elements that may be disclosed pursuant to this section, to include disclosure of ABO blood type and rh factor for the purpose of identifying or locating suspects, fugitives, material witnesses or missing persons. We agree with the commenters that these pieces of information are important to law enforcement investigations and are no more invasive of privacy than the other pieces of protected health information that may be disclosed under this provision.

However, as explained below, protected health information associated with DNA and DNA analysis; dental records; or typing, samples or analyses of tissues and bodily fluids other than blood (*e.g.,* saliva) cannot be disclosed for the location and identification purposes described in this section. Allowing disclosure of this information is not necessary to accomplish the purpose of this provision, and would be substantially more intrusive into individuals' privacy. In addition, we understand commenters' concern about the potential for such information to be compiled in law enforcement data bases. Allowing disclosure of such information could make individuals reluctant to seek care out of fear that health information about them could be compiled in such a data base.

Comment: Many commenters argued that proposed § 164.510(f)(2) should be deleted because it would permit law enforcement to engage in ''fishing expeditions'' or to create large data bases that could be searched for suspects and others.

Response: Some of this fear may have stemmed from the inclusion of the phrase ''other distinguishing characteristic''—which could be construed broadly—in the list of items that could have been disclosed pursuant to this section. In the final rule, we delete the phrase ''other distinguishing characteristic'' from the list of items that can be disclosed pursuant to § 164.512(f)(2). In its place, we allow disclosure of a description of distinguishing physical characteristics, such as scars, tattoos, height, weight, gender, race, hair and eye color, and the presence or absence of facial hair such as a beard or moustache. We believe that such a change, in addition to the changes described in the paragraph above, responds to commenters' concern that the NPRM would have allowed creation of a government data base of personal identifying information. Further, this modification provides additional guidance to covered entities regarding the type of information that may be disclosed under this provision.

Comment: At least one commenter recommended removing social security numbers (SSNs) from the list of items that may be disclosed pursuant to proposed § 164.510(f)(2). The commenter was concerned that including SSNs in the (f)(2) list would cause law enforcement agencies to demand that providers collect SSNs. In addition, the commenter was concerned that allowing disclosure of SSNs could lead to theft of identity by unscrupulous persons in policy departments and health care organizations.

Response: We disagree. We believe that on balance, the potential benefits from use of SSNs for this purpose outweigh the potential privacy intrusion from such use of SSNs. For example, SSNs can help law enforcement officials identify suspects are using aliases.

Comments Regarding Proposed § 164.510(f)(3), Information About a Victim of Crime or Abuse

Comment: Some law enforcement organizations expressed concern that proposed § 164.510(f)(3) could inhibit compliance with state mandatory reporting laws.

Response: We recognize that the NPRM could have preempted such state mandatory reporting laws, due to the combined impact of proposed §§ 164.510(m) and 164.510(f). As explained in detail in § 164.512(a) above, we did not intend that result, and we modify the final rule to make clear that this rule does not preempt state mandatory reporting laws.

Comment: Many commenters, including consumer and provider groups, expressed concern that allowing covered entities to disclose protected health information without authorization to law enforcement regarding victims of crime, abuse, and other harm could endanger victims, particularly victims of domestic violence, who could suffer further abuse if their abuser learned that the information had been reported. Provider groups also expressed concern about undermining provider-patient relationships. Some law enforcement representatives noted that in many cases, health care providers' voluntary reports of abuse or harm can be critical for the successful prosecution of violent crime. They argued, that by precluding providers from voluntarily reporting to law enforcement evidence of potential abuse, the proposed rule could make it more difficult to apprehend and prosecute criminals.

Response: We recognize the need for heightened sensitivity to the danger facing victims of crime in general, and victims of domestic abuse or neglect in particular. As discussed above, the final rule includes a new section (§ 164.512(c)) establishing strict conditions for disclosure of protected health information about victims of abuse, neglect, and domestic violence.

Victims of crime other than abuse, neglect, or domestic violence can also be placed in further danger by disclosure of protected health information relating to the crime. In § 164.512(f)(3) of the final rule, we establish conditions for disclosure of protected health information in these circumstances, and we make significant modifications to the proposed rule's provision for such disclosures. Under the final rule, unless a state or other

government authority has enacted a law requiring disclosure of protected health information about a victim to law enforcement officials, in most instances, covered entities must obtain the victim's agreement before disclosing such information to law enforcement officials. This requirement gives victims control over decision making about their health information where their safety could be at issue, helps promote trust between patients and providers, and is consistent with health care providers' ethical obligation to seek patient authorization whenever possible before disclosing protected health information.

At the same time, the rule strikes a balance between protecting victims and providing law enforcement access to information about potential crimes that cause harm to individuals, by waiving the requirement for agreement in two situations. In allowing covered entities to disclose protected health information about a crime victim pursuant to a state or other mandatory reporting law, we defer to other governmental bodies' judgments on when certain public policy objectives are important enough to warrant mandatory disclosure of protected health information to law enforcement. While some mandatory reporting laws are written more broadly than others, we believe that it is neither appropriate nor practicable to distinguish in federal regulations between what we consider overly broad and sufficiently focused mandatory reporting laws.

The final rule waives the requirement for agreement if the covered entity is unable to obtain the individual's agreement due to incapacity or other emergency circumstance, and (1) the law enforcement official represents that the information is needed to determine whether a violation of law by a person other than the victim has occurred and the information is not intended to be used against the victim; (2) the law enforcement official represents that immediate law enforcement activity that depends on the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and (3) the covered entity determines, in the exercise of professional judgment, that the disclosure is in the individual's best interests. By allowing covered entities, in the exercise of professional judgment, to determine whether such disclosures are in the individual's best interests, the final rule recognizes the importance of the provider-patient relationship.

In addition, the final rule allows covered entities to initiate disclosures of protected health information about victims without the victim's permission to law enforcement officials only if such disclosure is required under a state mandatory reporting law. In other circumstances, plans and providers may disclose protected health information only in response to a request from a law enforcement official. We believe that such an approach recognizes the importance of promoting trust between victims and their health care providers. If providers could initiate reports of victim information to law enforcement officials absent a legal reporting mandate, victims may avoid give their providers health information that could facilitate their treatment, or they may avoid seeking treatment completely.

Comment: Many commenters believed that access to medical records pursuant to this provision should occur only after judicial review. Others believed that it should occur only with patient consent or after notifying the patient of the disclosure to law enforcement. Similarly, some commenters said that the minimum necessary standard should apply to this provision, and they recommended restrictions on law enforcement agencies' re-use of the information.

Response: As discussed above, the final rule generally requires individual agreement as a condition for disclosure of a victim's health information; this requirement provides greater privacy protection and individual control than would a requirement for judicial review. We also discuss above the situations in which this requirement for agreement may be waived, and why that is appropriate. The requirement that covered entities disclose the minimum necessary protected health information consistent with the purpose of the disclosure applies to disclosures of protected health information about victims to law enforcement, unless the disclosure is required by law. (See § 164.514 for more detail on the requirements for minimum necessary use and disclosure of protected health information.) As described above, HIPAA does not provide statutory authority for HHS to regulate law enforcement agencies' re-use of protected health information that they obtain pursuant to this rule.

Comment: A few commenters expressed concern that the NPRM would not have required law enforcement agencies' requests for protected health information about victims to be in writing. They believed that written requests could promote clarity in law enforcement requests, as well as greater accountability among law enforcement officials seeking information.

Response: We do not impose this requirement in the final rule. We believe that such a requirement would not provide significant new protection for victims and would unduly impede the completion of legitimate law enforcement investigations.

Comment: A provider group was concerned that it would be difficult for covered entities to evaluate law enforcement officials' claims that information is needed and that law enforcement activity may be necessary. Some comments from providers and individuals expressed concern that the proposed rule would have provided open-ended access by law enforcement to victims' medical records because of this difficulty in evaluating law enforcement claims of their need for the information.

Response: We modify the NPRM in several ways that reduce covered entities' decisionmaking burdens. The final rule clarifies that covered entities may disclose protected health information about a victim of crime where a report is required by state or other law, and it requires the victim's agreement for disclosure in most other instances. The covered entity must make the decision whether to disclose only in limited circumstances: when there is no mandatory reporting law; or when the victim is unable to provide agreement and the law enforcement official represents that: the protected health information is needed to determine whether a violation of law by a person other than the victim has occurred, that the information will not be used against the victim, and that immediate law enforcement activity that depends on such information would be materially and adversely affected by waiting until the individual is able to agree to the disclosure. In these circumstances, we believe it is appropriate to rely on the covered entity, in the exercise of professional judgment, to determine whether the disclosure is in the individual's best interests. Other sections of this rule allow covered entities to reasonably rely on certain representations by law enforcement officials (see § 164.514, regarding verification,) and require disclosure of the minimum necessary protected health information for this purpose. Together, these provisions do not allow open-ended access or place undue responsibility on providers.

Comments Regarding Proposed § 164.510(f)(4), Intelligence and National Security Activities

In the final rule, we recognize that disclosures for intelligence and national security activities do not always involve

law enforcement. Therefore, we delete the provisions of proposed § 164.510(f)(4), and we address disclosures for intelligence and national security activities in § 164.512(k), on uses and disclosures for specialized government functions. Comments and responses on these issues are included below, in the comments for that section.

Comments Regarding Proposed § 164.510(f)(5), Health Care Fraud, Crimes on the Premises, and Crimes Witnessed by the Covered Entity's Workforce

Comment: Many commenters noted that proposed § 164.510(f)(5)(i), which covered disclosures for investigations and prosecutions of health care fraud, overlapped with proposed § 164.510(c) which covered disclosures for health oversight activities.

Response: As discussed more fully in § 164.512(d) of this preamble, above, we agree that proposed § 164.510(f)(5)(i) created confusion because all disclosures covered by that provision were already permitted under proposed § 164.510(c) without prior process. In the final rule, therefore, we delete proposed § 164.510(f)(5)(i).

Comment: One commenter was concerned the proposed provision would not have allowed an emergency room physician to report evidence of abuse when the suspected abuse had not been committed on the covered entity's premises.

Response: Crimes on the premises are only one type of crime that providers may report to law enforcement officials. The rules for reporting evidence of abuse to law enforcement officials are described in § 164.512(c) of the rule, and described in detail in § 164.512(c) of the preamble. An emergency room physician may report evidence of abuse if the conditions in § 164.512(c) are met, regardless of where the abuse occurred.

Comment: One commenter argued that covered entities should be permitted to disclose information that ''indicates the potential existence'' of evidence, not just information that ''constitutes evidence'' of crimes on the premises or crimes witnessed by a member of the covered entity's workforce.

Response: We agree that covered entities should not be required to guess correctly whether information will be admitted to court as evidence. For this reason, we include a good-faith standard in this provision. Covered entities may disclose information that it believes in good faith constitutes evidence of a crime on the premises. If the covered entity discloses protected health information in good faith but is wrong in its belief that the information is evidence of a violation of law, the covered entity will not be subject to sanction under this regulation.

Section 164.512(g)—Uses and Disclosures About Decedents

Coroners and Medical Examiners

Comment: We received several comments, for example, from state and county health departments, a private foundation, and a provider organization, in support of the NPRM provision allowing disclosure without authorization to coroners and medical examiners.

Response: The final rule retains the NPRM's basic approach to disclosure of coroners and medical examiners. It allows covered entities to disclose protected health information without authorization to coroners and medical examiners, for identification of a deceased person, determining cause of death, or other duties authorized by law.

Comment: In the preamble to the NPRM, we said we had considered but rejected the option of requiring covered entities to redact from individuals' medical records any information identifying other persons before disclosing the record to a coroner or medical examiner. We solicited comment on whether health care providers routinely identify other persons specifically in an individual's medical record and if so, whether in the final rule we should require health care providers to redact information about the other person before providing it to a coroner or medical examiner.

A few commenters said that medical records typically do not include information about persons other than the patient. One commenter said that patient medical records occasionally reference others such as relatives or employers. These commenters recommended requiring redaction of such information in any report sent to a coroner or medical examiner. On the other hand, other commenters said that redaction should not be required. These commenters generally based their recommendation on the burden and delay associated with redaction. In addition to citing the complexity and time involved in redaction of medical records provided to coroners, one commenter said that health plans and covered health care providers were not trained to determine the identifiable information necessary for coroners and medical examiners to do thorough investigations. Another commenter said that redaction should not be required because coroners and medical examiners needed some additional family information to determine what would be done with the deceased after their post-mortem investigation is completed.

Response: We recognize the burden associated with redacting medical records to remove the names of persons other than the patient. In addition, as stated in the preamble to the NPRM, we recognize that there is a limited time period after death within which an autopsy must be conducted. We believe that the delay associated with this burden could make it impossible to conduct a post-mortem investigation within the required time frame. In addition, we agree that health plans and covered health care providers may lack the training necessary to determine the identifiable information necessary for coroners and medical examiners to do thorough investigations. Thus, in the final rule, we do not require health plans or covered providers to redact information about persons other than the patient who may be identified in a patient's medical record before disclosing the record to a coroner or medical examiner.

Comment: One commenter said that medical records sent to coroners and medical examiners were considered their work product and thus were not released from their offices to anyone else. The commenter recommended that HHS establish regulations on how to dispose of medical records and that we create a ''no re-release'' statement to ensure that individual privacy is maintained without compromising coroners' or medical examiners' access to protected health information. The organization said that such a policy should apply regardless of whether the investigation was civil or criminal.

Response: HIPAA does not provide HHS with statutory authority to regulate coroners' or medical examiners' re-use or re-disclosure of protected health information unless the coroner or medical examiner is also a covered entity. However, we consistently have supported comprehensive privacy legislation to regulate disclosure and use of individually identifiable health information by all entities that have access to it.

Funeral Directors

Comment: One commenter recommended modifying the proposed rule to allow disclosure without authorization to funeral directors. To accomplish this change, the commenter suggested either: (1) Adding another subsection to proposed § 164.510 of the NPRM, to allow disclosure without authorization to funeral directors as needed to make arrangements for

funeral services and for disposition of a deceased person's remains; or (2) revising proposed § 164.510(e) to allow disclosure of protected health information to both coroners and funeral directors. According to this commenter, funeral directors often need certain protected health information for the embalming process, because a person's medical condition may affect the way in which embalming is performed. For example, the commenter noted, funeral directors increasingly receive bodies after organ and tissue donation, which has implications for funeral home staff duties associated with embalming.

Response: We agree with the commenter. In the final rule, we permit covered entities to disclose protected health information to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to a decedent. When necessary for funeral directors to carry out their duties, covered entities may disclose protected health information prior to and in reasonable anticipation of the individual's death.

Comment: One commenter recommended clarifying in the final rule that it does not restrict law enforcement agencies' release of medical information that many state records laws require to be reported, for example, as part of autopsy reports. The commenter recommended stating that law enforcement officials may independently gather medical information, that such information would not be covered by these rules, and that it would continue to be covered under applicable state and federal access laws.

Response: HIPAA does not give HHS statutory authority to regulate law enforcement officials' use or disclosure of protected health information. As stated elsewhere, we continue to support enactment of comprehensive privacy legislation to cover disclosure and use of all individually identifiable health information.

Comment: One commenter recommended prohibiting health plans and covered health care providers from disclosing psychotherapy notes to coroners or medical examiners.

Response: We disagree with the commenter who asserted that psychotherapy notes should only be used by or disclosed to coroners and medical examiners with authorization. Psychotherapy notes are sometimes needed by coroners and medical examiners to determine cause of death, such as in cases where suicide is suspected as the cause of death. We understand that several states require the disclosure of protected health information, including psychotherapy notes, to medical examiners and coroners. However, in the absence of a state law requiring such disclosure, we do not intend to prohibit coroners or medical examiners from obtaining the protected health information necessary to determine an individual's cause of death.

Section 164.512(h)—Uses and Disclosures for Organ Donation and Transplantation Purposes

Comment: Commenters noted that under the organ donation system, information about a patient is disclosed before seeking consent for donation from families. These commenters offered suggestions for ensuring that the system could continue to operate without consent for information sharing with organ procurement organizations and tissue banks. Commenters suggested that organ and tissue procurement organizations should be ''covered entities'' or that the procurement of organs and tissues be included in the definition of health care operations or treatment, or in the definition of emergency circumstances.

Response: We agree that organ and tissue donation is a special situation due to the need to protect potential donors' families from the stress of considering whether their loved one should be a donor before a determination has been made that donation would be medically suitable. Rather than list the entities that are ''covered entities'' or modify the definitions of health care operations and treatment or emergency circumstances to explicitly include organ procurement organizations and tissue banks, we have modified § 164.512 to permit covered entities to use or disclose protected health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissues.

Comment: Commenters asked that the rule clarify that organ procurement organizations are health care providers but not business partners of the hospitals.

Response: We agree that organ procurement organizations and tissue banks are generally not business associates of hospitals.

Disclosures and Uses for Government Health Data Systems

Comment: We received a number of comments supporting the exception for disclosure of protected health information to government health data systems. Some supporters stated a general belief that the uses of such information were important to improve and protect the health of the public. Commenters said that state agencies used the information from government health data systems to contribute to the improvement of the health care system by helping prevent fraud and abuse and helping improve health care quality, efficiency, and cost-effectiveness. Commenters asserted that state agencies take action to ensure that data they release based on these data systems do not identify individuals

We also received a large volume of comments opposed to the exception for use and disclosure of protected health information for government health data systems. Many commenters expressed general concern that the provision threatened their privacy, and many believed that their health information would be subject to abuse by government employees. Commenters expressed concern that the provision would facilitate collection of protected health information in one large, centralized government health database that could threaten privacy. Others argued that the proposed rule would facilitate law enforcement access to protected health information and could, in fact, become a database for law enforcement use.

Many commenters asserted that this provision would make individuals concerned about confiding in their health care providers. Some commenters argued that the government should not be allowed to collect individually identifiable health information without patient consent, and that the government could use de-identified data to perform the public policy analyses. Many individual commenters said that HHS lacked statutory and Constitutional authority to give the government access and control of their medical records without consent.

Many commenters believed that the NPRM language on government health data systems was too broad and would allow virtually any government collection of data to be covered. They argued that the government health data system exception was unnecessary because there were other provisions in the proposed rules providing sufficient authority for government agencies to obtain the information they need.

Some commenters were concerned that the NPRM's government health data system provisions would allow disclosure of protected health information for purposes unrelated to health care. These commenters recommended narrowing the provision to allow disclosure of protected health

information without consent to government health data systems in support of health care-related policy, planning, regulatory, or management functions. Others recommended narrowing the exception to allow use and disclosure of protected health information for government health databases only when a specific statute or regulation has authorized collection of protected health information for a specific purpose.

Response: We agree with the commenters who suggested that the proposed provision that would have permitted disclosures to government health data bases was overly broad, and we remove it from the final rule.

We reviewed the important purposes identified in the comments for government access to protected health information, and believe that the disclosures of protected health information that should appropriately be made without individuals' authorization can be achieved through the other disclosures provided for in the final rule, including provisions permitting covered entities to disclose information (subject to certain limitations) to government agencies for public health, research, health oversight, law enforcement, and otherwise as required by law. For example, the final rule continues to allow a covered entity to disclose protected health information without authorization to a public health authority to monitor trends in the spread of infectious disease, morbidity, and mortality. Under the rule's health oversight provision, covered entities can continue to disclose protected health information to public agencies for purposes such as analyzing the cost and quality of services provided by covered entities; evaluating the effectiveness of federal, state, and local public programs; examining trends in health insurance coverage of the population; and analyzing variations in access to health coverage among various segments of the population. We believe that it is better to remove the proposed provision for government health data systems generally and to rely on other, more narrowly tailored provisions in the rule to authorize appropriate disclosures to government agencies.

Comment: Some provider groups, private companies, and industry organizations recommended expanding the exception for government health data systems to include data collected by private entities. These commenters said that such an expansion would be justified, because private entities often perform the same functions as public agencies collecting health data.

Response: We eliminate the exception for government health data systems because it was over broad and the uses and disclosures we were trying to permit are permitted by other provisions. We note that private organizations may use or disclose protected health information pursuant to multiple provisions of the rule.

Comment: One commenter recommended clarifying in the final rule that the government health data system provisions apply to: (1) Manufacturers providing data to HCFA and its contractors to help the agency make reimbursement and related decisions; and to (2) third-party payors that must provide data collected by device manufacturers to HCFA to help the agency make reimbursement and related decisions.

Response: The decision to eliminate the general provision permitting disclosures to government health data systems makes this issue moot with respect to such disclosures. We note that the information used by manufacturers to support coverage determinations often is gathered pursuant to patient authorization (as part of informed consent for research) or as an approved research project. There also are many cases in which information can be de-identified before it is disclosed. Where HCFA hires a contractor to collect such protected health information, the contractor may do so under HCFA's authority, subject to the business associate provisions of this rule.

Comment: One commenter recommended stating in the final rule that de-identified information from government health data systems can be disclosed to other entities.

Response: HHS does not have the authority to regulate re-use or re-disclosure of information by agencies or institutions that are not covered entities under the rule. However, we support the policies and procedures that public agencies already have implemented to de-identify any information that they redisclose, and we encourage the continuation of these activities.

Disclosures for Payment Processes

Proposed § 164.510(j) of the NPRM would have allowed disclosure of protected health information without authorization for banking and payment processes. In the final rule, we eliminate this provision. Disclosures that would have been allowed under it, as well as comments received on proposed § 164.510(j), are addressed under § 164.501 of the final rule, under the definition of ''payment.''

Section 164.512(i)—Uses and Disclosures for Research Purposes

Documentation Requirements of IRB or Privacy Board Approval of Waiver

Comment: A number of commenters argued that the proposed research requirements of § 164.510(j) exceeded the Secretary's authority under section 246(c) of HIPAA. In particular, several commenters argued that the Department was proposing to extend the Common Rule and the use of the IRB or privacy boards beyond federally-funded research projects, without the necessary authority under HIPAA to do so. One commenter stated that, ''Section 246(c) of HIPAA requires the Secretary to issue a regulation setting privacy standards for individually identifiable health information transmitted in connection with the transactions described in section 1173(a),'' and thus concluded that the disclosure of health information to researchers is not covered. Some of these commenters also argued that the documentation requirements of proposed § 164.510(j), did not shield the NPRM from having the effect of regulating research by placing the onus on covered health care providers to seek documentation that certain standards had been satisfied before providing protected health information to researchers. These commenters argued that the proposed rule had the clear and intended effect of directly regulating researchers who wish to obtain protected health information from a covered entity.

Response: As discussed above, we do not agree with commenters that the Secretary's authority is limited to individually identifiable health information transmitted in connection with the transactions described in section 1173(a) of HIPAA. We also disagree that the proposed research documentation requirements would have constituted the unauthorized regulation of researchers. The proposed requirements established conditions for the use of protected health information by covered entities for research and the disclosure of protected health information by covered entities to researchers. HIPAA authorizes the Secretary to regulate such uses and disclosures, and the final rule retains documentation requirements similar to those proposed.

Comment: Several commenters believed that the NPRM was proposing either directly or indirectly to modify the Common Rule and, therefore, stated that such modification was beyond the Secretary's authority under HIPAA. Many of these commenters arrived at this conclusion because the waiver of

authorization criteria proposed in § 164.510(j) differed from the Common Rule's criteria for the waiver of informed consent (Common Rule, § .116(d)).

Response: We do not agree that the proposed provision relating to research would have modified the Common Rule. The provisions that we proposed and provisions that we include in the final rule place conditions that must be met before a covered entity may use or disclose protected health information. Those conditions are in addition to any conditions required of research entities under the Common Rule. Covered entities will certainly be subject to laws and regulations in addition to the rule, but the rule does not require compliance with these other laws or regulations. For covered health care providers and health plans that are subject to both the final rule and the Common Rule, both sets of regulations will need to be followed.

Comment: A few commenters suggested that the Common Rule should be extended to all research, regardless of funding source.

Response: We generally agree with the commenters on the need to provide protections to all human subjects research, regardless of funding source. HIPAA, however, did not provide the Department with authority to extend the Common Rule beyond its current purview. For research that relies on the use or disclosure of protected health information by covered entities without authorization, the final rule applies the Common Rule's principles for protecting research subjects by, in most instances, requiring documentation of independent board review, and a finding that specified criteria designed to protect the privacy of prospective research subjects have been met.

Comment: A large number of commenters agreed that the research use and disclosure of protected health information should not require authorization. Of these commenters, many supported the proposed rule's approach to research uses and disclosures without authorization, including many from health care provider organizations, the mental health community, and members of Congress. Others, while they agreed that the research use and disclosure should not require authorization disagreed with the NPRM's approach and proposed alternative models.

The commenters who supported the NPRM's approach to permitting researchers access to protected health information without authorization argued that it was appropriate to apply ''Common Rule-like'' provisions to privately funded research. In addition, several commenters explicitly argued that the option to use a privacy board, in lieu of an IRB, must be maintained because requiring IRB review to include all aspects of patient privacy could diffuse focus and significantly compromise an IRB's ability to execute its primary patient protection role. Furthermore, several commenters believed that privacy board review should be permitted, but wanted equal oversight and accountability for privacy boards and IRBs.

Many other commenters agreed that the research use and disclosure should not require authorization, but disagreed with the proposed rule's approach and proposed alternative models. Several of these commenters argued that the final rule should eliminate the option for privacy board review and that all research to be subject to IRB review. These commenters stated that having separate and unequal systems to approve research based on its funding source would complicate compliance and go against the spirit of the regulations. Several of these commenters, many from patient and provider organizations, opposed the permitted use of privacy boards to review research studies and instead argued that IRB review should be required for all studies involving the use or disclosure of protected health information. These commenters argued that although privacy board requirements would be similar, they are not equitable; for example, only three of the Common Rule's six requirements for the membership of IRBs were proposed to be required for the membership on privacy boards, and there was no proposed requirement for annual review of ongoing research studies that used protected health information. Several commenters were concerned that the proposed option to obtain documentation of privacy board review, in lieu of IRB review, would perpetuate the divide in the oversight of federally-funded versus publically-funded research, rather than eliminate the differential oversight of publically-and privately-funded research, with the former still being held to a stricter standard. Some of these commenters argued that these unequal protections would be especially apparent for the disclosure of research with authorization, since under the Common Rule, IRB review of human subjects studies is required, regardless of the subject's consent, before the study may be conducted.

Response: Although we share the concern raised by commenters that the option for the documentation of privacy board approval for an alteration or waiver of authorization may perpetuate the unequal mechanisms of protecting the privacy of human research subjects for federally-funded versus publically-funded research, the final rule is limited by HIPAA to addressing only the use and disclosure of protected health information by covered entities, not the protection of human research subjects more generally. Therefore, the rule cannot standardize human subjects protections throughout the country. Given the limited scope of the final rule with regard to research, the Department believes that the option to obtain documentation of privacy board approval for an alteration or waiver of authorization in lieu of IRB approval provides covered entities with needed flexibility. Therefore, in the final rule we have retained the option for covered entities to rely on documentation of privacy board approval that specified criteria have been met.

We disagree with the rationale suggested by commenters who argued that the option for privacy board review must be maintained because requiring IRB review to include all aspects of patient privacy could diffuse focus and significantly compromise an IRB's ability to execute its primary patient protection role. For research that involves the use of individually identifiable health information, assessing the risk to the privacy of research subjects is currently one of the key risks that must be assessed and addressed by IRBs. In fact, we expect that it will be appropriate for many research organizations that have existing IRBs to rely on these IRBs to meet the documentation requirements of § 164.512(i).

Comment: One health care provider organization recommended that the IRB or privacy board mechanism of review should be applied to non-research uses and disclosures.

Response: We disagree. Imposing documentation of privacy board approval for other public policy uses and disclosures permitted by § 164.512 would result in undue delays in the use or disclosure of protected health information that could harm individuals and the public. For example, requiring that covered health care providers obtain third-party review before permitting them to alert a public health authority that an individual was infected with a serious communicable disease could cause delay appropriate intervention by a public health authority and could present a serious threat to the health of many individuals.

Comment: A number of commenters, including several members of Congress,

argued that since the research provisions in proposed § 164.510(j) were modeled on the existing system of human subjects protections, they were inadequate and would shatter public trust if implemented. Similarly, some commenters, asserted that IRBs are not accustomed to reviewing and approving utilization reviews, outcomes research, or disease management programs and, therefore, IRB review may not be an effective tool for protecting patient privacy in connection with these activities. Some of these commenters noted that proposed § 164.510(j) would exacerbate the problems inherent in the current federal human subjects protection system especially in light of the recent GAO reports that indicate the IRB system is already over-extended. Furthermore, a few commenters argued that the Common Rule's requirements may be suited for interventional research involving human subjects, but is ill suited to the archival and health services research typically performed using medical records without authorization. Therefore, these commenters concluded that extending ''Common Rule-like'' provisions to the private sector would be inadequate to protect human subjects and would result in significant and unnecessary cost increases.

Response: While the vast majority of government-supported and regulated research adheres to strict protocols and the highest ethical standards, we agree that the federal system of human subjects protections can and must be strengthened. To work toward this goal, on May 23, the Secretary announced several additional initiatives to enhance the safety of subjects in clinical trials, strengthen government oversight of medical research, and reinforce clinical researchers' responsibility to follow federal guidelines. As part of this initiative, the National Institutes of Health have undertaken an aggressive effort to ensure IRB members and IRB staff receive appropriate training in bioethics and other issues related to research involving human subjects, including research that involves the use of individually identifiable health information. With these added improvements, we believe that the federal system of human subjects protections continues to be a good model to protect the privacy of individually identifiable health information that is used for research purposes. This model of privacy protection is also consistent with the recent recommendations of both the Institute of Medicine in their report entitled, ''Protecting Data Privacy in Health Services Research,'' and the Joint Commission on Accreditation of Healthcare Organizations and the National Committee for Quality Assurance in their report entitled, ''Protecting Personal Health Information: A Framework for Meeting the Challenges in a Managed Care Environment.'' Both of these reports similarly concluded that health services research that involves the use of individually identifiable health information should undergo IRB review or review by another board with sufficient expertise in privacy and confidentiality protection.

Furthermore, it is important to recognize that the Common Rule applies not only to interventional research, but also to research that uses individually identifiable health information, including archival research and health services research. The National Bioethics Advisory Commission (NBAC) is currently developing a report on the federal oversight of human subjects research, which is expected to address the unique issues raised by non-interventional human subjects research. The Department looks forward to receiving NBAC's report, and carefully considering the Commission's recommendations. This final rule is the first step in enhancing patients' privacy and we will propose modifications to the rule if changes are warranted by the Commission's findings and recommendations.

Comment: Many commenters argued that the proposed research provision would have a chilling affect on the willingness of health plans and covered providers to participate in research because of the criminal and civil penalties that could be imposed for failing to meet the requirements that would have been required by proposed § 164.510(j). Some of these commenters cautioned, that over time, research could be severely hindered if covered entities choose not to disclose protected health information to researchers. In addition, one commenter recommended that a more reasonable approach would be to require IRB or privacy board approval only if the results of the research were to be broadly published. Another commenter expressed concern that the privacy rule could influence IRBs or privacy boards to refuse to recognize the validity of decisions by other IRBs or privacy boards and specifically recommended that the privacy rule include a preamble statement that: (1) The ''risk'' balancing consider only the risk to the patient, not the risk to the institution, and (2) add a phrase that the decision by the initial IRB or privacy board to approve the research shall be given deference by other IRBs or privacy boards. This commenter also recommended that to determine whether IRBs or privacy boards were giving such deference to prior IRB or privacy board review, HHS should monitor the disapproval rate by IRB or privacy boards conducting secondary reviews.

Response: As the largest federal sponsor of medical research, we understand the important role of research in improving our Nation's health. However, the benefits of research must be balanced against the risks, including the privacy risks, for those who participate in research. An individual's rights and welfare must never be sacrificed for scientific or medical progress. We believe that the requirements for the use and disclosure of protected health information for research without authorization provides an appropriate balance. We understand that some covered health care providers and health plans may conclude that the rule's documentation requirements for research uses and disclosures are too burdensome.

We rejected the recommendation that documentation of IRB or privacy board approval of the waiver of authorization should only be required if the research were to be ''broadly published.'' Research findings that are published in de-identified form have little influence on the privacy interests of individuals. We believe that it is the use or disclosure of individually identifiable health information to a researcher that poses the greater risk to individuals' privacy, not publication of de-identified information.

We agree with the commenters that IRB or privacy board review should address the privacy interests of individuals and not institutions. This provision is intended to protect individuals from unnecessary uses and disclosures of their health information and does not address institutional privacy.

We disagree with the comment that documentation of IRB or privacy board approval of the waiver of authorization should be given deference by other IRBs or privacy boards conducting secondary reviews. We do not believe that it is appropriate to restrict the deliberations or judgments of privacy boards, nor do we have the authority under this rule to instruct IRBs on this issue. Instead, we reiterate that all disclosures for research purposes under § 164.512(i) are voluntary, and that institutions may choose to impose more stringent requirements for any use and disclosure permitted under § 164.512.

Comment: Some commenters were concerned about the implications of proposed § 164.510(j) on multi-center research. These commenters argued that for multi-center research, researchers may require protected health information from multiple covered entities, each of whom may have different requirements for the documentation of IRB or privacy board review. Therefore, there was concern that documentation that may suffice for one covered entity, may not for another, thereby hindering multi-center research.

Response: Since § 164.512(i) establishes minimum documentation standards for covered health care providers and health plans using or disclosing protected health information for research purposes, we understand that some covered providers and health plans may choose to require additional documentation requirements for researchers. We note, however, that nothing in the final rule would preclude a covered health care provider or health plan from developing the consistent documentation requirements provided they meet the requirements of § 164.512(i).

Comment: One commenter who was also concerned that the minimum necessary requirements of proposed § 164.506(b) would negatively affect multi-center research because covered entities participating in multi-site research studies would no longer be permitted to rely upon the consent form approved by a central IRB, and nor would participating entities be permitted to report data to the researcher using the case report form approved by the central IRB to guide what data points to include. This commenter noted that the requirement that each site would need to undertake a separate minimum necessary review for each disclosure would erect significant barriers to the conduct of research and may compromise the integrity and validity of data combined from multiple sites. This commenter recommended that the Secretary absolve a covered entity of the responsibility to make its own individual minimum necessary determinations if the entity is disclosing information pursuant to an IRB or privacy board-approved protocol.

Response: The minimum necessary requirements in the final rule have been revised to permit covered entities to rely on the documentation of IRB or privacy board approval as meeting the minimum necessary requirements of § 164.514. However, we anticipate that much multi-site research, such as multi-site clinical trials, will be conducted with patients' informed consent as required by the Common Rule and FDA's protection of human subjects regulations, and that patients' authorization will also be sought for the use or disclosure of protected health information for such studies. Therefore, it should be noted that the minimum necessary requirements do not apply for uses or disclosures made with an authorization. In addition, the final rule allows a covered health care provider or health plan to use or disclose protected health information pursuant to an authorization that was approved by a single IRB or privacy board, provided the authorization met the requirements of § 164.508. The final rule does not, however, require IRB or privacy board review for the use or disclosure of protected health information for research conducted with individuals' authorization.

Comment: Some commenters believed that proposed § 164.510(j) would have required documentation of both IRB and privacy board review before a covered entity would be permitted to disclose protected health information for research purposes without an individual's authorization.

Response: This is incorrect. Section 164.512(i)(1)(i) of the final rule requires documentation of alteration or waiver approval by either an IRB or a privacy board.

Comment: Some commenters believed that the proposed rule would have required that patients be notified whenever protected health information about themselves was disclosed for research purposes.

Response: This is incorrect. Covered entities are not required to inform individuals that protected health information about themselves has been disclosed for research purposes. However, as required in § 164.520 of the final rule, the covered entity must include research disclosures in their notice of information practices. In addition, as required by § 164.528 of the rule, covered health care providers and health plans must provide individuals, upon request, with an accounting of disclosures made of protected health information about the individual.

Comment: One commenter recommended that IRB and privacy boards also be required to be accredited.

Response: While we agree that the issue of accrediting IRBs and privacy boards deserves further consideration, we believe it is premature to require covered entities to ensure that the IRB or privacy board that approves an alteration or waiver of authorization is accredited. Currently, there are no accepted accreditation standards for IRBs or privacy boards, nor a designated accreditation body. Recognizing the need for and value of greater uniformity and public accountability in the review and approval process, HHS, with support from the Office of Human Research Protection, National Institutes of Health, Food and Drug Administration, Centers for Disease Control and Prevention, and Agency for Health Care Research and Quality, has engaged the Institute of Medicine to recommend uniform performance resource-based standards for private, voluntary accreditation of IRBs. This effort will draw upon work already undertaken by major national organizations to develop and test these standards by the spring of 2001, followed by initiation of a formal accreditation process before the end of next year. Once the Department has received the Institute of Medicine's recommended accreditation standards and process for IRBs, we plan to consider whether this accreditation model would also be applicable to privacy boards.

Comment: A few commenters also noted that if both an IRB and a privacy board reviewed a research study and came to conflicting decisions, proposed § 164.510(j) was unclear about which board's decision would prevail.

Response: The final rule does not stipulate which board's decision would prevail if an IRB and a privacy board came to conflicting decisions. The final rule requires covered entities to obtain documentation that one IRB or privacy board has approved of the alteration or waiver of authorization. The covered entity, however, has discretion to request information about the findings of all IRBs and/or privacy boards that have reviewed a research proposal. We strongly encourage researchers to notify IRBs and privacy boards of any prior IRB or privacy board review of a research protocol.

Comment: Many commenters noted that the NPRM included no guidance on how the privacy board should approve or deny researchers' requests. Some of these commenters recommended that the regulation stipulate that privacy boards be required to follow the same voting rules as required under the Common Rule.

Response: We agree that the Common Rule (§ __.108(b)) provides a good model of voting procedures for privacy boards and incorporate such procedures to the extent they are relevant. In the final rule, we require that the documentation of alteration or waiver of authorization state that the alteration or waiver has been reviewed and approved by either (1) an IRB that has followed the voting requirements of the Common Rule (§ __.108(b)), or the expedited review

procedures of the Common Rule (§ __.110); or (2) unless an expedited review procedure is used, a privacy board that has reviewed the proposed research at a convened meeting at which a majority of the privacy board members are present, including at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any such entities, and the alteration or waiver of authorization is approved by the majority of privacy board members present at the meeting.

Comment: A few commenters were concerned that the research provisions would be especially onerous for small non-governmental entities, furthering the federal monopoly on research.

Response: We understand that the documentation requirements of § 164.512(i), as well as other provisions in the final rule, may be more onerous for small entities than for larger entities. We believe, however, that when protected health information is to be used or disclosed for research without an individual's authorization, the additional privacy protections in § 164.512(i) are essential to reduce the risk of harm to the individual.

Comment: One commenter believed that it was paradoxical that, under the proposed rule, the disclosure of protected health information for research conducted with an authorization would have been more heavily burdened than research that was conducted without authorization, which they reasoned was far less likely to bring personal benefit to the research subjects.

Response: It was not our intent to impose more requirements on covered entities using or disclosing protected health information for research conducted with authorization than for research conducted without authorization. In fact, the proposed rule would have required only authorization as stipulated in proposed § 164.508 for research disclosures made with authorization, and would have been exempt from the documentation requirements in proposed § 164.510(j). We retain this treatment in the final rule. We disagree with the commenter who asserted that the requirements for research conducted with authorization are more burdensome for covered health care providers and plans than the documentation provisions of this paragraph.

Comment: A number of comments, mostly from the pharmaceutical industry, recommended that the final rule state that privacy boards be permitted to waive authorization only with respect to research uses of medical information collected in the course of treatment or health care operations, and not with respect to clinical research. Similarly, one commenter recommended that IRBs and privacy boards be authorized to review privacy issues only, not the entire research project. These commenters were concerned that by granting waiver authority to privacy boards and IRBs, and by incorporating the Common Rule waiver criteria into the waiver criteria included in the proposed rule, the Secretary has set the stage for privacy boards to review and approve waivers in circumstances that involve interventional research that is not subject to the Common Rule.

Response: We agree with the commenters who recommended that the final rule clarify that the documentation of IRB or privacy board approval of the waiver of authorization would be based only on an assessment of the privacy risks associated with a research study, not an assessment of all relevant risks to participants. In the final rule, we have amended the language in the waiver criteria to make clear that these criteria relate only to the privacy interests of the individual. We anticipate, however, that the vast majority of uses and disclosures of protected health information for interventional research will be made with individuals' authorization. Therefore, we expect it will be rare that a researcher will seek IRB or privacy board approval for the alteration or waiver of authorization, but seek informed consent for participation for the interventional component of the research study. Furthermore, we believe that interventional research, such as most clinical trials, could not meet the waiver criteria in the final rule (§ 164.512(i)(2)(ii)(C)), which states ''the research could not practicably be conducted without the alteration or waiver.'' If a researcher is to have direct contact with research subjects, the researcher should in virtually all cases be able to seek and obtain patients' authorization for the use and disclosure of protected health information about themselves for the research study.

Comment: A few commenters recommended that the rule explicitly state that covered entities would be permitted to rely upon an IRB or privacy boards' representation that the research proposal meets the requirements of proposed § 164.510(j).

Response: We agree with this comment. The final rule clarifies that covered health care providers and health plans are allowed to rely on an IRB's or privacy board's representation that the research proposal meets the requirements of § 164.512(i).

Comment: One commenter recommended that IRBs be required to maintain web sites with information on proposed and approved projects.

Response: We agree that it could be useful for IRBs and privacy boards to maintain web sites with information on proposed and approved projects. However, requiring this of IRBs and privacy boards is beyond the scope of our authority under HIPAA. In addition, this recommendation raises concerns that would need to be addressed, including concerns about protecting the confidentiality of research participants and propriety information that may be contained in research proposals. For these reasons, we decided not to incorporate this requirement into the final rule.

Comment: One commenter recommended that HHS collect data on research-related breaches of confidentiality and investigate existing anecdotal reports of such breaches.

Response: This recommendation is beyond HHS' legal authority, since HIPAA did not give us the authority to regulate researchers. Therefore, this recommendation was not included in the final rule.

Comment: A number of commenters were concerned that HIPAA did not give the Secretary the authority to protect information once it was disclosed to researchers who were not covered entities.

Response: The Secretary shares these commenters' concerns about the Department's limited authority under HIPAA. We strongly support the enactment of additional federal legislation to fill these crucial gaps in the Secretary's authority.

Comment: One commenter recommended that covered entities should be required to retain the IRB's or privacy board's documentation of approval of the waiver of individuals' authorization for at least six years from when the waiver was obtained.

Response: We agree with this comment and have included such a requirement in the final rule. See § 164.530(j).

Comment: One commenter recommended that whenever health information is used for research or administrative purposes, a plan is in place to evaluate whether to and how to feed patient-specific information back into the health system to benefit an individual or group of patients from whom the health information was derived.

Response: While we agree that this recommendation is consistent with the

responsible conduct of research, HIPAA did not give us the authority to regulate research. Therefore, this recommendation was not included in the final rule.

Comment: A few commenters recommended that contracts between covered entities and researcher be pursued. Comments received in favor of requiring contractual agreements argued that such a contract would be enforceable under law, and should prohibit secondary disclosures by researchers. Some of these commenters recommended that contracts between covered entities and researchers should be the same as, or modeled on, the proposed requirements for business partners. In addition, some commenters argued that contracts between covered entities and researchers should be required as a means of placing equal responsibility on the researcher for protecting protected health information and for not improperly re-identifying information.

Response: In the final rule, we have added an additional waiver criteria to require that there are adequate written assurances from the researcher that protected health information will not be re-used or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of protected health information would be permitted by this subpart. We believe that this additional waiver criteria provides additional assurance that protected health information will not be misused by researchers, while not imposing the additional burdens of a contractual requirement on covered health care providers and health plans. We were not persuaded by the comments received that contractual requirements would provide necessary additional protections, that would not also be provided by the less burdensome waiver criteria for adequate written assurance that the researcher will not re-use or disclose protected health information, with few exceptions. Our intent was to strengthen and extend existing privacy safeguards for protected health information that is used or disclosed for research, while not creating unnecessary disincentives to covered health care providers and health plans who choose to use or disclose protected health information for research purposes.

Comment: Some commenters explicitly opposed requiring contracts between covered entities and researchers as a condition of permitting the use or disclosure of protected health information for research purposes. These commenters argued that such a contractual requirement would be too onerous for covered entities and researchers and would hinder or halt important research.

Response: We agree with the arguments raised by these commenters, and thus, the final rule does not require contracts between covered entities and researchers as a condition of using or disclosing protected health information for research purposes without authorization.

Comment: A large number of commenters strongly supported requiring patient consent before protected health information could be used or disclosed, including but not limited to use and disclosure for research purposes. These commenters argued that the unconsented-to use of their medical records abridged their autonomy right to decide whether or not to participate in research. A few referenced the Nuremberg Code in support of their view, noting that the Nuremberg Code required individual consent for participation in research.

Response: We agree that it is of foremost importance that individuals' privacy rights and welfare be safeguarded when protected health information about themselves is used or disclosed for research studies. We also strongly believe that continued improvements in the nation's health requires that researchers be permitted access to protected health information without authorization in certain circumstances. Additional privacy protections are needed, however, and we have included several in the final rule. If covered entities plan to disclose protected health without individuals' authorization for research purposes, individuals must be informed of this through the covered entity's notice to patients of their information practices. In addition, before covered health care providers or health plans may use or disclose protected health information for research without authorization, they must obtain documentation that an IRB or privacy board has found that specified waiver criteria have been met, unless the research will include protected health information about deceased individuals only, or is solely for reviews that are preparatory to research.

While it is true that the first provision of the Nuremberg Code states that ''the voluntary consent of the human subject is absolutely essential,'' it is important to understand the context of this important document in the history of protecting human subjects research from harm. The Nuremberg Code was developed for the Nuremberg Military Tribunal as standards by which to judge the human experimentation conducted by the Nazis, and was one of the first documents setting forth principles for the ethical conduct of human subjects research. The acts of atrocious cruelty that the Nuremberg Code was developed to address, focused on preventing the violations to human rights and dignity that occurred in the name of ''medical advancement.'' The Code, however, did not directly address the ethical conduct of non-interventional research, such as medical records research, where the risk of harm to participants can be unlike those associated with clinical research.

We believe that the our proposed requirements for the use or disclosure of protected health information for research are consistent with the ethical principles of ''respect for persons,'' ''beneficence,'' and ''justice,'' which were established by the Belmont Report in 1978, and are now accepted as the quintessential requirements for the ethical conduct of research involving human subjects, including research using individually identifiable health information. These ethical principles formed the foundation for the requirements in the Common Rule, on which our proposed requirements for research uses and disclosures were modeled.

Comment: Many commenters recommended that the privacy rule permit individuals to opt out of having their records used for the identified ''important'' public policy purposes in § 164.510, including for research purposes. These commenters asserted that permitting the use and disclosure of their protected health information without their consent, or without an opportunity to ''opt out'' of having their information used or disclosed, abridged individuals' right to decide who should be permitted access to their medical records. In addition, one commenter argued that although the research community has been sharply critical of a Minnesota law that limits access to health records (Minnesota Statute Section 144.335 (1998)), researchers have cited a lack of response to mailed consent forms as the primary factor behind a decrease in the percentage of medical records available for research. This commenter argued that an opt-out provision would not be subject to this ''nonresponder'' problem.

Response: We believe that a meaningful right to ''opt out'' of a research study requires that individuals be contacted and informed about the study for which protected health information about themselves is being requested by a researcher. We concluded, therefore, that an ''opt out'' provision of this nature may suffer from

the same decliner bias that has been experienced by researchers who are subject to laws that require patient consent for medical records research. Furthermore, evidence on the effect of a mandatory ''opt out'' provision for medical records research is only fragmentary at this time, but at least one study has preliminarily suggested that those who refuse to consent for research access to their medical records may differ in statistically significant ways from those who consent with respect to variables such as age and disease category (SJ Jacobsen et al. ''Potential Effect of Authorization Bias on Medical Records Research.'' Mayo Clin Proc 74: (1999) 330–338). For these reasons, we disagree with the commenters who recommended that an ''opt out'' provision be included in the final rule. In the final rule, we do require covered entities to include research disclosures in their notice of information practices. Therefore, individuals who do not wish for protected health information about themselves to be disclosed for research purposes without their authorization could select a health care provider or health plan on this basis. In addition, the final rule also permits covered health care providers or health plans to agree not to disclose protected health information for research purposes, even if research disclosures would otherwise be permitted under their notice of information practices. Such an agreement between a covered health care provider or health plan and an individual would not be enforceable under the final rule, but might be enforceable under applicable state law.

Comment: Some commenters explicitly recommended that there should be no provision permitting individuals to opt out of having their information used for research purposes.

Response: We agree with these commenters for the reasons discussed above.

IRB and Privacy Board Review

Comments: The NPRM imposed no requirements for the location or sponsorship of the IRB or privacy board. One commenter supported the proposed approach to permit covered entities to rely on documentation of a waiver by a IRB or privacy board that was convened by the covered entity, the researcher, or another entity.

In contrast, a few commenters recommended that the NPRM require that the IRB or privacy board be outside of the entity conducting the research, although the rationale for these recommendations was not provided. Several industry and consumer groups alternatively recommended that the regulation require that privacy boards be based at the covered entity. These comments argued that ''if the privacy board is to be based at the entity receiving data, and that entity is not a covered entity, there will be little ability to enforce the regulation or study the effectiveness of the standards.''

Response: We agree with the comment supporting the proposed rule's provision to impose no requirements for the location or sponsorship of the IRB or privacy board that was convened to review a research proposal for the alteration or waiver of authorization criteria. In the absence of a rationale, we were not persuaded by the comments asserting that the IRB or privacy board should be convened outside of the covered entity. In addition, while we agree with the comments that asserted HHS would have a greater ability to enforce the rule if a privacy board was established at the covered entity rather than an uncovered entity, we concluded that the additional burden that such a requirement would place on covered entities was unwarranted. Furthermore, under the Common Rule and FDA's protection of human subjects regulations, IRB review often occurs at the site of the recipient researchers' institution, and it was not our intent to change this practice. Therefore, in the final rule, we continue to impose no requirements for the location or sponsorship of the IRB or privacy board.

Privacy Board Membership

Comment: Some commenters were concerned that the proposed composition of the privacy board did not adequately address potential conflicts of interest of the board members, particularly since the proposed rule would have permitted the board's ''unaffiliated'' member to be affiliated with the entity disclosing the protected health information for research purposes. To address this concern, some commenters recommended that the required composition of privacy boards be modified to require ''* * * at least one member who is not affiliated with the entity receiving or disclosing protected health information.'' These commenters believed that this addition would be more sound and more consistent with the Common Rule's requirements for the composition of IRBs. Furthermore, it was argued that this requirement would prohibit covered entities from creating a privacy board comprised entirely of its own employees.

Response: We agree with these comments. In the final rule we have revised the proposed membership for privacy board to reduce potential conflict of interest among board members. The final rule requires that documentation of alteration or waiver from a privacy board, is only valid under § 164.512(i) if the privacy board includes at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to a person who is affiliated with such entities.

Comment: One commenter recommended that privacy boards be required to include more than one unaffiliated member to address concerns about conflict of interest among members.

Response: We disagree that privacy boards should be required to include more than one unaffiliated member. We believe that the revised membership criterion for the unaffiliated member of the privacy board, and the criterion that requires that the board have no member participating in a review of any project in which the member has a conflict of interest, are sufficient to ensure that no member of the board has a conflict of interest in a research proposal under their review.

Comment: Many commenters also recommended that the membership of privacy boards be required to be more similar to that of IRBs. These commenters were concerned that privacy boards, as described in the proposed rule, would not have the needed expertise to adequately review and oversee research involving the use of protected health information. A few of these commenters also recommended that IRBs be required to have at least one member trained in privacy or security matters.

Response: We disagree with the comments asserting that the membership of privacy boards should be required be more similar to IRBs. Unlike IRBs, privacy boards only have responsibility for reviewing research proposals that involve the use or disclosure of protected health information without authorization. We agree, however, that the proposed rule may not have ensured that the privacy board had the necessary expertise to protect adequately individuals' privacy rights and interests. Therefore, in the final rule, we have modified one of the membership criteria for privacy board to require that the board has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests.

Comment: Two commenters recommended that IRBs and privacy

boards be required to include patient advocates.

Response: The Secretary's legal authority under HIPAA does not permit HHS to modify the membership of IRBs. Moreover, we disagree with the comments recommending that IRBs and privacy board should be required to include patient advocates. We were not persuaded that patient advocates are the only persons with the needed expertise to protect patients' privacy rights and interests. Therefore, in the final rule, we do not require that patient advocates be included as members of a privacy board. However, under the final rule, IRBs and privacy board members could include patient advocates provided they met the required membership criteria in § 164.512(i).

Comment: A few commenters requested clarification of the term ''conflict of interest'' as it pertained to the proposed rule's criteria for IRB and privacy board membership. In particular, some commenters recommended that the final rule clarify what degree of involvement in a research project by a privacy board member would constitute a conflict, thereby precluding that individual's participation in a review. One commenter specifically requested clarification about whether employment by the covered entity constituted a conflict of interest, particularly if the covered entity is receiving a financial gain from the conduct of the research.

Response: We understand that determining what constitutes conflict of interest can be complex. We do not believe that employees of covered entities or employees of the research institution requesting protected health information for research purposes are necessarily conflicted, even if those employees may benefit financially from the research. However, there are many factors that should be considered in assessing whether a member of an IRB has a conflict of interest, including financial and intellectual conflicts.

As part of a separate, but related effort to the final rule, during the summer of 2000, HHS held a conference on human subject protection and financial conflicts of interest. In addition, HHS solicited comments from the public about financial conflicts of interest associated with human subjects research for researchers, IRB members and staff, and research sponsors. The findings from the conference and the public comments received are forming the basis for guidance that HHS is now developing on financial conflicts of interest.

Privacy Training for IRB and Privacy Boards

Comment: A few commenters expressed support for training IRB members and chairs about privacy issues, recommending that such training either be required or that it be encouraged in the final rule.

Response: We agree with these comments and thus encourage institutions that administer IRBs and privacy boards to ensure that the members of these boards are adequately trained to protect the privacy rights and welfare of individuals about whom protected health information is used for research purposes. In the final rule, we require that privacy board members have varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests. We believe that this criterion for privacy board membership requires that members already have the necessary knowledge or that they be trained to address privacy issues that arise in the conduct of research that involves the use of protected health information. In addition, we note that the Common Rule (§ .107(a)) already imposes a general requirement that IRB members posses adequate training and experience to adequately evaluate the research which it reviews. IRBs are also authorized to obtain the services of consultants (§ .107(f)) to provide expertise not available on the IRB. We believe that these existing requirements in the Common Rule already require that an IRB have the necessary privacy expertise.

Waiver Criteria

Comment: A large number of comments supported the proposed rule's criteria for the waiver of authorization by an IRB or privacy board.

Response: While we agree that several of the waiver criteria should be retained in the final rule, we have made changes to the waiver criteria to address some of the comments we received on specific criteria. These reason for these changes are discussed in the response to comments below.

Comment: In addition to the proposed waiver criteria, several commenters recommended that the final rule also instruct IRBs and privacy boards to consider the type of protected health information and the sensitivity of the information to be disclosed in determining whether to grant a waiver, in whole or in part, of the authorization requirements.

Response: We agree with these comments, but believe that the requirement to consider the type and sensitivity of protected health information was already encompassed by the proposed waiver criteria. We encourage and expect that IRBs and privacy boards will take into consideration the type and sensitivity of protected health information, as appropriate, in considering the waiver criteria included in the final rule.

Comment: Many commenters were concerned that the criteria were not appropriate in the context of privacy risks and recommended that the waiver criteria be rewritten to more precisely focus on the protection of patient privacy. In addition, some commenters argued that the proposed waiver criteria were redundant with the Common Rule and were confusing because they mix elements of the Common Rule's waiver criteria—some of which they argued were relevant only to interventional research. In particular, a number of commenters raised these concerns about proposed criterion (ii). Some of these commenters suggested that the word ''privacy'' be inserted before ''rights.''

Response: We agree with these comments. To focus all of the criterion on individuals' privacy interests, in the final rule, we have modified one of the proposed waiver criteria, eliminated one proposed criterion, and added an additional criterion : (1) the proposed criterion which stated, ''the waiver will not adversely affect the rights and welfare of the subjects,'' has been revised in the final rule as follows: ''the alteration or waiver will not adversely affect the privacy rights and the welfare of the individuals;'' (2) the proposed criterion which stated, ''whenever appropriate, the subjects will be provided with additional pertinent information after participation,'' has been eliminated; and (3) a criterion has been added in the final rule which states, ''there are adequate written assurances that the protected health information will not be re-used or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of protected health information would be permitted by this subpart.'' In addressing these criteria, we expect that IRBs and privacy boards will not only consider the immediate privacy interests of the individual that would arise from the proposed research study, but also the possible implications from a loss of privacy, such as the loss of employment, loss or change in cost of health insurance, and social stigma.

Comment: A number of commenters were concerned about the interaction between the proposed rule and the Common Rule. One commenter opposed the four proposed waiver criteria which differed from the Common Rule's criteria for the waiver of informed consent (§ .116(d)) on the grounds that the four criteria proposed in addition to the Common Rule's waiver criteria would apply only to the research use and disclosure of protected health information by covered entities. This commenter argued that this would lead to different standards for the protection of other kinds of individually identifiable health information used in research that will fall outside of the scope of the final rule. This commenter concluded that this inconsistency would be difficult for IRBs to administer, difficult for IRB members to distinguish, and would be ethically questionable. For these reasons, many commenters recommended that the final rule should permit the waiver criteria of the Common Rule, to be used in lieu of the waiver criteria identified in the proposed rule.

Response: We disagree with the comments recommending that the waiver criteria of the Common Rule should be permitted to be used in lieu of the waiver criteria identified in the proposed rule. The Common Rule's waiver criteria were designed to protect research subjects from all harms associated with research, not specifically to protect individuals' privacy interests. We understand that the waiver criteria in the final rule may initially cause confusion for IRBs and researchers that must attend to both the final rule and the Common Rule, but we believe that the additional waiver criteria adopted in the final rule are essential to ensure that individuals' privacy rights and welfare are adequately safeguarded when protected health information about themselves is used for research without their authorization. We agree that ensuring that the privacy rights and welfare of all human subjects—involved in all forms of research—is ethically required, and the new Office of Human Research Protection will immediately initiate plans to review the confidentiality provisions of the Common Rule.

In addition, at the request of the President, the National Bioethics Advisory Commission has begun an examination of the current federal human system for the protection of human subjects in research. The current scope of the federal regulatory protections for protecting human subjects in research is just one of the issues that will be addressed in the by the Commission's report, and the Department looks forward to receiving the Commission's recommendations.

Concerns About Specific Waiver Criteria

Comment: One commenter argued that the term ''welfare'' was vague and recommended that it be deleted from the proposed waiver of authorization criterion which stated, ''the waiver will not adversely affect the rights and welfare of the subjects.''

Response: We disagree with the comment recommending that the final rule eliminate the term ''welfare'' from this waiver criterion. As discussed in the National Bioethics Advisory Commission's 1999 report entitled, ''Research Involving Human Biological Materials: Ethical Issues and Policy Guidance,'' ''Failure to obtain consent may adversely affect the rights and welfare of subjects in two basic ways. First, the subject may be improperly denied the opportunity to choose whether to assume the risks that the research presents, and second, the subject may be harmed or wronged as a result of his or her involvement in research to which he or she has not consented * * *. Subjects' interest in controlling information about themselves is tied to their interest in, for example, not being stigmatized and not being discriminated against in employment and insurance.'' Although this statement by the Commission was made in the context of research involving human biological materials, we believe research that involves the use of protected health information similarly requires that social and psychological harms be considered when assessing whether an alteration or waiver will adversely affect the privacy rights and welfare of individuals. We believe it would be insufficient to attend only to individuals' privacy ''rights'' since some of the harms that could result from a breach of privacy, such as stigmatization, and discrimination in employment or insurance, may not be tied directly to an individuals' ''rights,'' but would have a significant impact on their welfare. Therefore, in the final rule, we have retained the term ''welfare'' in this criterion for the alteration or waiver of authorization but modified the criterion as follows to focus more specifically on privacy concerns and to clarify that it pertains to alterations of authorization: ''the alteration or waiver will not adversely affect the privacy rights and the welfare of the individual.''

Comment: A few commenters recommended that the proposed waiver criteria that stated, ''the research could not practicably be conducted without the waiver,'' be modified to eliminate the term ''practicably.'' These commenters believed that determining ''practicably'' was subjective and that its elimination would facilitate IRBs' and privacy boards' implementation of this criterion. In addition, one commenter was concerned that this term could be construed to require authorization if enough weight is given to a privacy interest, and little weight is given to cost or administrative burden. This commenter recommended that the criterion be changed to allow a waiver if the ''disclosure is necessary to accomplish the research or statistical purpose for which the disclosure is to be made.''

Response: We disagree with the comments recommending that the term ''practicability'' be deleted from this waiver criterion. We believe that an assessment of practicability is necessary to account for research that may be possible to conduct with authorization but that would be impracticable if authorization were required. For example, in research study that involves thousands of records, it may be possible to track down all potential subjects, but doing so may entail costs that would make the research impracticable. In addition, IRBs have experience implementing this criterion since it is nearly identical to a waiver criterion in the Common Rule (§ __.116(d)(3)).

We also disagree with the recommendation to change the criterion to state, ''disclosure is necessary to accomplish the research or statistical purpose for which the disclosure is to be made.'' We believe it is essential that consideration be given as to whether it would be practicable for research to be conducted with authorization in determining whether a waiver of authorization is justified. If the research could practicably be conducted with authorization, then authorization must be sought. Authorization must not be waived simply for convenience.

Therefore, in the final rule, we have retained this criterion and clarified that it also applies to alterations of authorization. This waiver criterion in the final rule states, ''the research could not practicably be conducted without the alteration or waiver.''

Comment: Some commenters argued that the criterion which stated, ''whenever appropriate, the subjects will be provided with additional pertinent information after participation,'' should be deleted. Some comments recommended that the criterion should be deleted for privacy reasons, arguing that it would be inappropriate to create a reason for the researcher to contact the individual

whose data were analyzed, without IRB review of the proposed contact as a patient intervention. Other commenters argued for the deletion of the criterion on grounds that requiring researchers to contact patients whose records were used for archival research would be unduly burdensome, while adding little to the patient's base of information. Several commenters also argued that the criterion was not pertinent to non-interventional retrospective research requiring access to archived protected health information.

In addition, one commenter asserted that this criterion was inconsistent with the Secretary's rationale for prohibiting disclosures of ''research information unrelated to treatment'' for purposes other than research. This commenter argued that the privacy regulations should not mandate that a covered entity provide information with unknown validity or utility directly to patients. This commenter recommended that a patient's physician, not the researcher, should be the one to contact a patient to discuss the significance of new research findings for that individual patient's care.

Response: Although we disagree with the arguments made by commenters recommending that this criterion be eliminated in the final rule, we concluded that the criterion was not directly related to ensuring the privacy rights and welfare of individuals. Therefore, we eliminated this criterion in the final rule.

Comment: A few commenters recommended that the criterion, which required that ''the research would be impracticable to conduct without access to and use of the protected health information,'' be deleted because it would be too subjective to be meaningful.

Response: We disagree with comments asserting that this proposed criterion would be too subjective. We believe that researchers should be required to demonstrate to an IRB or privacy board why protected health information is necessary for their research proposal. If a researcher could practicably use de-identified health information for a research study, protected health information should not be used or disclosed for the study without individuals' authorization. Therefore, we retain this criterion in the final rule. In considering this criterion, we expect IRBs and privacy boards to consider the amount of information that is needed for the study. To ensure the covered health care provider or health plan is informed of what information the IRB or privacy board has determined may be used or disclosed without authorization, the final rule also requires that the documentation of IRB or privacy board approval of the alteration or waiver describe the protected health information for which use or access has been determined to be necessary.

Comment: A large number of comments objected to the proposed waiver criterion, which stated that, ''the research is of sufficient importance so as to outweigh the intrusion of the privacy of the individual whose information is subject to the disclosure.'' The majority of these commenters argued that the criterion was overly subjective, and that due to its subjectivity, IRBs and privacy boards would inevitably apply it inconsistently. Several commenters asserted that this criterion was unsound in that it would impose on reviewing bodies the explicit requirement to form and debate conflicting value judgments about the relative weights of the research proposal versus an individual's right to privacy. Furthermore these commenters argued that this criterion was also unnecessary because the Common Rule already has a requirement that deals with this issue more appropriately. In addition, one commenter argued that the rule eliminate this criterion because common purposes should not override individual rights in a democratic society. Based on these arguments, these commenters recommended that this criterion be deleted.

Response: We disagree that it is inappropriate to ask IRBs and privacy boards to ensure that there is a just balance between the expected benefits and risks to individual participants from the research. As noted by several commenters, IRBs currently conduct such a balancing of risks and benefits because the Common Rule contains a similar criterion for the approval of human subjects research (§ __.111(a)(2)). However, we disagree with the comments asserting that the proposed criterion was unnecessary because the Common Rule already contains a similar criterion. The Common Rule does not explicitly address the privacy interests of research participants and does not apply to all research that involves the use or disclosure of protected health information. However, we agree that the relevant Common Rule criterion for the approval of human subjects research provides better guidance to IRBs and privacy boards for assessing the privacy risks and benefits of a research proposal. Therefore, in the final rule, we modeled the criterion on the relevant Common Rule requirement for the approval of human subjects research, and revised the proposed criterion to state: ''the privacy risks to individuals whose protected health information is to be used or disclosed are reasonable in relation to the anticipated benefits if any to the individuals, and the importance of the knowledge that may reasonably be expected to result from the research.''

Comment: One commenter asserted that as long as the research organization has adequate privacy protections in place to keep the information from being further disclosed, it is unnecessary for the IRB or privacy board to make a judgment on whether the value of the research outweighs the privacy intrusion.

Response: The Department disagrees with the assertion that adequate safeguards of protected health information are sufficient to ensure that the privacy rights and welfare of individuals are adequately protected. We believe it is imperative that there be an assessment of the privacy risks and anticipated benefits of a research study that proposes to use protected health information without authorization. For example, if a research study was so scientifically flawed that it would provide no useful knowledge, any risk to patient privacy that might result from the use or disclosure of protected health information without individuals' authorization would be too great.

Comment: A few commenters asserted that the proposed criterion requiring ''an adequate plan to destroy the identifiers at the earliest opportunity consistent with the conduct of the research, unless there is a health or research justification for retaining identifiers,'' conflicted with the regulations of the FDA on clinical record keeping (21 CFR 812.140(d)) and the International Standard Organization on control of quality records (ISO 13483, 4.16), which require that relevant data be kept for the life of a device.

In addition, one commenter asserted that this criterion could prevent follow up care. Similarly, other commenters argued that the new waiver criteria would be likely to confuse IRBs and may impair researchers' ability to go back to IRBs to request extensions of time for which samples or data can be stored if researchers are unable to anticipate future uses of the data.

Response: We do not agree with the comment that there is a conflict between either the FDA or the ISO regulations and the proposed waiver criteria in the rule. We believe that compliance with such recordkeeping requirements would be ''consistent with the conduct of research'' which is subject to such requirements. Nonetheless, to avoid any confusion, in the final rule we have added the phrase ''or such retention is

otherwise required by law'' to this waiver criterion.

We also disagree with the comments that this criterion would prevent follow up care to individuals or unduly impair researchers from retaining identifiers on data for future research. We believe that patient care would qualify as a ''health * * * justification for retaining identifiers.'' In addition, we understand that researchers may not always be able to anticipate that the protected health information they receive from a covered health care provider or health plan for one research project may be useful for the conduct of future research studies. However, we believe that the concomitant risk to patient privacy of permitting researchers to retain identifiers they obtained without authorization would undermine patient trust, unless researchers could identify a health or research justification for retaining the identifiers. In the final rule, an IRB or privacy board is not required to establish a time limit on a researcher's retention of identifiers.

Additional Waiver Criteria

Comment: A few comments recommended that there be a additional waiver criterion to safeguard or limit subsequent use or disclosure of protected health information by the researcher.

Response: We agree with these comments. In the final rule, we include a waiver criterion requiring ''there are adequate written assurances that the protected health information will not be re-used or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of protected health information would be permitted by this subpart.''

Waiving Authorization, in Whole or in Part

Comment: A few commenters requested that the final rule clarify what ''in whole or in part'' means if authorization is waived or altered.

Response: In the proposed rule, it was HHS' intent to permit IRBs and privacy boards to either waive all of the elements for authorization, or alternatively, waive only some of the elements of authorization. Furthermore, we also intended to permit IRBs and privacy boards to alter the authorization requirements. Therefore, in the final rule, we clarify that the alteration to and waiver of authorization, in whole or in part, are permitted as stipulated in § 164.512(i).

Expedited Review

Comment: One commenter asserted that the proposed rule would prohibit expedited review as permitted under the Common Rule. Many commenters supported the proposal in the rule to incorporate the Common Rule's provision for expedited review, and strongly recommended that this provision be retained in the final rule. Several of these commenters argued that the expedited review mechanism provides IRBs with the much-needed flexibility to focus volunteer-IRB members' limited resources.

Response: We agree that expedited review should be available, and included a provision permitting expedited review under specified conditions. We understand that the National Bioethics Advisory Commission is currently developing a report on the federal oversight of human subjects research, which is expected to address the Common Rule's requirements for expedited review. HHS looks forward to receiving the National Bioethics Advisory Commission's report, and will modify the provisions for expedited review in the privacy rule if changes are warranted by the Commission's findings and recommendations.

Required Signature

Comment: A few commenters asserted that the proposed requirement that the written documentation of IRB or privacy board approval be signed by the chair of the IRB or the privacy board was too restrictive. Some commenters recommended that the final rule permit the documentation of IRB or privacy board approval to be signed by persons other than the IRB or privacy board chair, including: (1) Any person authorized to exercise executive authority under IRB's or privacy board's written procedures; (2) the IRB's or privacy board's acting chair or vice chair in the absence of the chair, if permitted by IRB procedures; and (3) the covered entity's privacy official.

Response: We agree with the commenters who argued that the final rule should permit the documentation of IRB or privacy board approval to be signed by someone other than the chair of the board. In the final rule, we permit the documentation of alteration or waiver of authorization to be signed by the chair or other member, as designated by the chair of the IRB or privacy board, as applicable.

Research Use and Disclosure With Authorization

Comment: Some commenters, including several industry and consumer groups, argued that the proposed rule would establish a two-tiered system for public and private research. Privately funded research conducted with an authorization for the use or disclosure of protected health information would not require IRB or privacy board review, while publically funded research conducted with authorization would require IRB review as required by the Common Rule. Many of these commenters argued that authorization is insufficient to protect patients involved in research studies and recommended that IRB or privacy board review should be required for all research regardless of sponsor. These commenters asserted that it is not sufficient to obtain authorization, and that IRBs and privacy boards should review the authorization document, and assess the risks and benefits to individuals posed by the research.

Response: For the reasons we rejected the recommendation that we eliminate the option for privacy board review and require IRB review for the waiver of authorization, we also decided against requiring documentation of IRB or privacy board approval for research conducted with authorization. HHS strongly agrees that IRB review is essential for the adequate protection of human subjects involved in research, regardless of whether informed consent and/or individuals' authorization is obtained. In fact, IRB review may be even more important for research conducted with subjects' informed consent and authorization since such research may present greater than minimal risk to participants. However, HHS' authority under HIPAA is limited to safeguarding the privacy of protected health information, and does not extend to protecting human subjects more broadly. Therefore, in the final rule we have not required documentation of IRB or privacy board review for the research use or disclosure of protected health information conducted with individuals' authorization. As mentioned above, HHS looks forward to receiving the recommendations of the National Bioethics Advisory Commission, which is currently examining the current scope of federal regulatory protections for protecting human subjects in research as part of its overarching report on the federal oversight of human subjects protections.

Comment: Due to concern about several of the elements of authorization, many commenters recommended that the final rule stipulate that ''informed consent'' obtained pursuant to the Common Rule be deemed to meet the requirements for ''authorization.'' These commenters argued that the NPRM's

additional authorization requirements offered no additional protection to research participants but would be a substantive impediment to research.

Response: We disagree with the comments asserting that the proposed requirements for authorization for the use or disclosure of protected health information would have offered research subjects no additional privacy protection. Because the purposes of authorization and informed consent differ, the proposed rule's requirements for authorization pursuant to a request from a researcher (§ 164.508) and the Common Rule's requirements for informed consent (Common Rule, § __.116) contain important differences. For example, unlike the Common Rule, the proposed rule would have required that the authorization include a description of the information to be used or disclosed that identifies the information in a specific and meaningful way, an expiration date, and where, use of disclosure of the requested information will result in financial gain to the entity, a statement that such gain will result. We believe that the authorization requirements provide individuals with information necessary to determine whether to authorize a specific use or disclosure of protected health information about themselves, that are not required by the Common Rule.

Therefore, in the final rule, we retain the requirement for authorization for all uses and disclosures of protected health information not otherwise permitted without authorization by the rule. Some of the proposed requirements for authorization were modified in the final rule as discussed in the preamble on § 164.508. The comments received on specific proposed elements of authorization as they would have pertained to research are addressed below.

Comment: A number of commenters, including several from industry and consumer groups, recommended that the final rule require patients' informed consent as stipulated in the Common Rule. These commenters asserted that the proposed authorization document was inadequate for research uses and disclosures of protected health information since it included fewer elements than required for informed consent under the Common Rule, including for example, the Common Rule's requirement that the informed consent document include: (1) A description of any reasonably foreseeable risks or discomforts to the subject; (2) a description of any benefits to the subject or to others which may reasonably be expected from the research (Common Rule, § __.116(a)).

Response: While we agree that the ethical conduct of research requires the voluntary informed consent of research subjects, as stipulated in the Common Rule, as we have stated elsewhere, the privacy rule is limited to protecting the confidentiality of individually identifiable health information, and not protecting human subjects more broadly. Therefore, we believe it would not be within the scope of the final rule to require informed consent as stipulated by the Common Rule for research uses and disclosures of protected health information.

Comment: Several commenters specifically objected to the authorization requirement for a ''expiration date.'' To remedy this concern, many of these commenters proposed that the rule exempt research from the requirement for an expiration date if an IRB has reviewed and approved the research study. In particular, some commenters asserted that the requirement for an expiration date would be impracticable in the context of clinical trials, where the duration of the study depends on several different factors that cannot be predicted in advance. These commenters argued that determining an exact date would be impossible due to the legal requirements that manufactures and the Food and Drug Administration be able to retrospectively audit the source documents when patient data are used in clinical trials. In addition, some commenters asserted that a requirement for an expiration date would force researchers to designate specific expiration dates so far into the future as to render them meaningless.

Response: We agree with commenters that an expiration date is not always possible or meaningful. In the final rule, we continue to require an identifiable expiration, but permit it to be a specific date or an event directly relevant to the individual or the purpose of the authorization *(e.g.,* for the duration of a specific research study) in which the individual is a participant.

Comment: A number of commenters, including those from the pharmaceutical industry, were concerned about the authorization requirement that gave patients the right to revoke consent for participation in clinical research. These commenters argued that such a right to revoke authorization for the use of their protected health information would require complete elimination of the information from the record. Some stated that in the conduct of clinical trials, the retrieval of individually identifiable health information that has already been blinded and anonymized, is not only burdensome, but should this become a widespread practice, would render the trial invalid. One commenter suggested that the Secretary modify the proposed regulation to allow IRBs or privacy boards to determine the duration of authorizations and the circumstances under which a research participant should be permitted to retroactively revoke his or her authorization to use data already collected by the researcher.

Response: We agree with these concerns. In the final rule we have clarified that an individual cannot revoke an authorization to the extent that action has been taken in reliance on the authorization. Therefore, if a covered entity has already used or disclosed protected health information for a research study pursuant to an authorization obtained as required by § 164.508, the covered entity is not required under the rule, unless it agreed otherwise, to destroy protected health information that was collected, nor retrieve protected health information that was disclosed under such an authorization. However, once an individual has revoked an authorization, no additional protected health information may be used or disclosed unless otherwise permitted by this rule.

Comment: Some commenters were concerned that the authorization requirement to disclose ''financial gain'' would be problematic as it would pertain to research. These commenters asserted that this requirement could mislead patients and would make it more difficult to attract volunteers to participate in research. One commenter recommended that the statement be revised to state ''that the clinical investigator will be compensated for the value of his/her services in administrating this clinical trial.'' Another commenter recommended that the authorization requirement for disclosure of financial gain be defined in accordance with FDA's financial disclosure rules.

Response: We strongly believe that a requirement for the disclosure of financial gain is imperative to ensure that individuals are informed about how and why protected health information about themselves will be used or disclosed. We agree, however, that the language of the proposed requirement could cause confusion, because most activities involve some type of financial gain. Therefore, in the final rule, we have modified the language to provide that when the covered entity initiates

the authorization and the covered entity will receive direct or indirect remuneration (rather than financial gain) from a third party in exchange for using or disclosing the health information, the authorization must include a statement that such remuneration will result.

Comment: A few commenters asserted that the requirement to include a statement in which the patient acknowledged that information used or disclosed to any entity other than a health plan or health care provider may no longer be protected by federal privacy law would be inconsistent with existing protections implemented by IRBs under the Common Rule. In particular they stated that this inconsistency exists because IRBs are required to consider the protections in place to protect patients' confidential information and that IRBs are charged with ensuring that researchers comply with the confidentiality provisions of the informed consent document.

Response: We disagree that this proposed requirement would pose a conflict with the Common Rule since the requirement was for a statement that the ''information may no longer be protected by the federal privacy law.'' This statement does not pertain to the protections provided under the Common Rule. In addition, while we anticipate that IRBs and privacy boards will most often waive all or none of the authorization requirements, we clarify an IRB or privacy board could alter this requirement, among others, if the documentation requirements of § 164.512(i) have been met.

Reviews Preparatory to Research

Comment: Some industry groups expressed concern that the research provision would prohibit physicians from using patient information to recruit subjects into clinical trials. These commenters recommended that researchers continue to have access to hospitals' and clinics' patient information in order to recruit patients for studies.

Response: Under the proposed rule, even if the researcher only viewed the medical record at the site of the covered entity and did not record the protected health information in a manner that patients could be identified, such an activity would have constituted a use or disclosure that would have been subject to proposed § 164.508 or proposed § 164.510. Based on the comments received and the fact finding we conducted with the research community, we concluded that documentation of IRB or privacy board approval could halt the development of research hypotheses that require access to protected health information before a formal protocol can be developed and brought to an IRB or privacy board for approval. To avoid this unintended result, the final rule permits covered health care providers and health plans to use or disclose protected health information for research if the covered entity obtains from the researcher representations that: (1) Use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research; (2) no protected health information is to be removed from the covered entity by the researcher in the course of the review; and (3) the protected health information for which use or access is sought is necessary for the research purposes.

Comment: A few commenters asserted that the final rule should eliminate the possibility that research requiring access to protected health information could be determined to be ''exempt'' from IRB review, as provided by the Common Rule (§ __.101(b)(4)).

Response: The rule did not propose nor intend to modify any aspect of the Common Rule, including the provision that exempts from coverage, ''research involving the collection or study of existing data, documents, records, pathological specimens, or diagnostic specimens, if these sources are publically available, or if the information is recorded by the investigator in such a manner that subjects cannot be identified, directly or indirectly through identifiers linked to the subjects' (§ __.101(b)(4)). For the reasons discussed above, we have included a provision in the final rule for reviews preparatory to research that was modeled on this exemption to the Common Rule.

Deceased Persons Exception for Research

Comment: A few commenters expressed support for the proposal to allow use and disclosure of protected health information about decedents for research purposes without the protections afforded to the protected health information of living individuals. One commenter, for example, explained that it extensively uses such information in its research, and any restrictions were likely to impede its efforts. Alternately, a number of commenters provided arguments for eliminating the research exception for deceased persons. They commented that the same concerns regarding use and disclosure of genetic and hereditary information for other purposes apply in the research context. They believed that in many cases the risk of identification was greater in the research context because researchers may attempt to identify genetic and hereditary conditions of the deceased. Finally, they argued that while information of the deceased does not necessarily identify living relatives by name, living relatives could be identified and suffer the same harm as if their own medical records were used or disclosed for research purposes. Another commenter stated that the exception was unnecessary, and that existing research could and should proceed under the requirements in proposed § 164.510 that dictated the IRB/privacy board approval process or be conducted using de-identified information. This commenter further stated that in this way, at least there would be some degree of assurance that all reasonable steps are taken to protect deceased persons' and their families' confidentiality.

Response: Although we understand the concerns raised by commenters, we believe those concerns are outweighed by the need to keep the research-related policies in this rule as consistent as possible with standard research practice under the Common Rule, which does not consider deceased persons to be ''human subjects.'' Thus, we retain the exception in the final rule. With regard to the protected health information about a deceased individual, therefore, a covered entity is permitted to use or disclose such information for research purposes without obtaining authorization from a personal representative and absent approval by an IRB or privacy board as governed by § 164.512(i). We note that the National Bioethics Advisory Committee (NBAC) is currently considering revising the Common Rule's definition of ''human subject'' with regard to coverage of the deceased. However, at this time, NBAC's deliberations on this issue are not yet completed and any reliance on such discussions would be premature.

The final rule requires at § 164.512(i)(1)(iii) that covered entities obtain from the researcher (1) representation that the use or disclosure is sought solely for research on the protected health information of decedents; (2) documentation, at the request of the covered entity, of the death of such individuals; and (3) representation that the protected health information for which use or disclosure is sought is necessary for the research purposes. It is our intention with this change to reduce the burden and ambiguity on the part of the covered entity to determine whether or not the

request is for protected health information of a deceased individual.

Comment: Some commenters, in their support of the research exception, requested that HHS clarify in the final rule that protected health information obtained during the donation process of eyes and eye tissue could continue to be used or disclosed to or by eye banks for research purposes without an authorization and without IRB approval. They expressed concern over the impediments to this type of research these approvals would impose, such as added administrative burden and vulnerabilities to the time sensitive nature of the process.

Another commenter similarly expressed the position that, with regard to uses and disclosures of protected health information for tissue, fluid, or organ donation, the regulation should not present an obstacle to the transfer of donations unsuitable for transplant to the research community. However, they believed that consent can be obtained for such purposes since the donor or donor's family must generally consent to any transplant purposes, it would seem to be a minimal additional obligation to seek consent for research purposes at the same time, should the material be unsuitable for transplant.

Response: Protected health information about a deceased individual, including information related to eyes and eye tissue, can be used or disclosed further for research purposes by a covered entity in accordance with § 164.512(i)(1)(iii) without authorization or IRB or privacy board approval. This rule does not address whether organs unsuitable for transplant may be transferred to researchers with or without consent.

Modification of the Common Rule

Comment: We received a number of comments that interpreted the proposed rule as having unnecessarily and inappropriately amended the Common Rule. Assuming that the Common Rule was being modified, these comments argued that the rule was legally deficient under the Administrative Procedures Act, the Regulatory Flexibility Act, and other controlling Executive orders or laws.

In addition, one research organization expressed concern that, by involving IRBs in the process of approving a waiver of authorization for disclosure purposes and establishing new criteria for such waiver approvals, the proposed rule would have subjected covered entities whose IRBs failed to comply with the requirements for reviewing and approving research to potential sanctions under HIPAA. The comment recommended that the rule be changed to eliminate such a punitive result. Specifically, the comment recommended that the existing Common Rule structure be preserved for IRB-approved research, and that the waiver of authorization criteria for privacy purposes be kept separate from the other functions of the IRB.

Response: We disagree with the comments asserting the proposed rule attempted to change the Common Rule. It was not our intent to modify or amend the Common Rule or to regulate the activities of the IRBs with respect to the underlying research. We therefore reject the comments about legal deficiencies in the rule which are based on the mistaken perception that the Common Rule was being amended. The proposed rule established new requirements for covered entities before they could use or disclose protected health information for research without authorization. The proposed rule provided that one method by which a covered entity could obtain the necessary documentation was to receive it from an IRB. We did not mandate IRBs to perform such reviews, and we expressly provided for means other than through IRBs for covered entities to obtain the required documentation.

In the final rule, we also have clarified our intent not to interfere with existing requirements for IRBs by amending the language in the waiver criteria to make clear that these criteria relate to the privacy interests of the individual and are separate from the criteria that would be applied by an IRB to any evaluation of the underlying research. Moreover, we have restructured the final rule to also make clear that we are regulating only the content and conditions of the documentation upon which a covered entity may rely in making a disclosure of protected health information for research purposes.

We cannot and do not purport to regulate IRBs or modify the Common Rule through this regulation. We cannot under this rule penalize an IRB for failure to comply with the Common Rule, nor can we sanction an IRB based on the documentation requirements in the rule. Health plans and covered health care providers may rely on documentation from an IRB or privacy board concerning the alteration or waiver of authorization for the disclosure of protected health information for research purposes, provided the documentation, on its face, meets the requirements in the rule. Health plans and covered health care providers will not be penalized for relying on facially adequate documentation from an IRB. Health plans and covered health providers will only be penalized for their own errors or omissions in following the requirements of the rule, and not those of the IRB.

Use Versus Disclosure

Comment: Many of the comments supported the proposed rule's provision that would have imposed the same requirements for both research uses and research disclosures of protected health information.

Response: We agree with these comments. In the final rule we retain identical use and disclosure requirements for research uses and disclosures of protected health information by covered entities.

Comment: In contrast, a few commenters recommended that there be fewer requirements on covered entities for internal research uses of protected health information.

Response: For the reasons discussed above in § 164.501 on the definition of ''research,'' we disagree that an individual's privacy interest is of less concern when covered entities use protected health information for research purposes than when covered entities disclose protected health information for research purposes. Therefore, in the final rule, the research-related requirements of § 164.512(i) apply to both uses and disclosures of protected health information for research purposes without authorization.

Additional Resources for IRBs

Comment: A few commenters recommended that HHS work to provide additional resources to IRBs to assist them in meeting their new responsibilities.

Response: This recommendation is beyond our statutory authority under HIPAA, and therefore, cannot be addressed by the final rule. However, we fully agree that steps should be taken to moderate the workload of IRBs and to ensure adequate resources for their activities. Through the Office for Human Research Protections, the Department is committed to working with institutions and IRBs to identify efficient ways to optimize utilization of resources, and is committed to developing guidelines for appropriate staffing and workload levels for IRBs.

Additional Suggested Requirements

Comment: One commenter recommended that the documentation of IRB or privacy board approval also be required to state that, ''the health researcher has fully disclosed which of

the protected health information to be collected or created would be linked to other protected health information, and that appropriate safeguards be employed to protect information against re-identification or subsequent unauthorized linkages.''

Response: The proposed provision for the use or disclosure of protected health information for research purposes without authorization only pertained to individually identifiable health information. Therefore, since the information to be obtained would be individually identifiable, we concluded that it was illogical to require IRBs and privacy boards document that the researcher had ''fully disclosed that * * * appropriate safeguards be employed to protect information against re-identification or subsequent unauthorized linkages.'' Therefore, we did not incorporate this recommendation into the final rule.

Section 164.512(j)—Uses and Disclosures To Avert a Serious Threat to Health or Safety

Comment: Several commenters generally stated support for proposed § 164.510(k), which was titled ''Uses and Disclosures in Emergency Circumstances.'' One commenter said that ''narrow exceptions to confidentiality should be permitted for emergency situations such as duty to warn, duty to protect, and urgent law enforcement needs.'' Another commented that the standard '' * * * based on a reasonable belief that the disclosures are necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual'' would apply in only narrow treatment circumstances. Some commenters suggested that the provision be further narrowed, for example, with language specifically identifying ''imminent threats'' and a ''chain-of-command clearance process,'' or by limiting permissible disclosures under this provision to ''public health emergencies,'' or ''national emergencies.'' Others proposed procedural requirements, such as specifying that such determinations may only be made by the patient's treating physician, a licensed mental health care professional, or as validated by three physicians. One commenter recommended stating that the rule is not intended to create a duty to warn or to disclose protected health information but rather permits such disclosure in emergency circumstances, consistent with other applicable legal or ethical standards.

Response: We agree with the commenters who noted that the proposed provision would apply in rare circumstances. We clarify, however, that we did not intend for the proposed provision to apply to emergency treatment scenarios as discussed below. In the final rule, to avoid confusion over the circumstances in which we intend this section to apply, we retitle it ''Uses and Disclosures to Avert a Serious Threat to Health or Safety.''

We do not believe it would be appropriate to narrow further the scope of permissible disclosures under this section to respond to specifically identified ''imminent threats,'' a ''public health emergency,'' or a ''national emergency.'' We believe it would be impossible to enumerate all of the scenarios that may warrant disclosure of protected health information pursuant to this section. Such cases may involve a small number of people and may not necessarily involve a public health emergency or a national emergency.

Furthermore, in response to comments arguing that the proposed provision was too broad, we note that under both the NPRM and the final rule, we allow but do not require disclosures in situations involving serious and imminent threats to health or safety. Health plans and covered health care providers may make the disclosures allowed under § 164.512(j) consistent with applicable law and standards of ethical conduct.

As indicated in the preamble to the NPRM, the proposed approach is consistent with statutory and case law addressing this issue. The most well-known case on the topic is Tarasoff v. Regents of the University of California, 17 Cal. 3d 425 (1976), which established a duty to warn those at risk of harm when a therapist's patient made credible threats against the physical safety of a specific person. The Supreme Court of California found that the therapist involved in the case had an obligation to use reasonable care to protect the intended victim of his patient against danger, including warning the victim of the peril. Many states have adopted, in statute or through case law, versions of the Tarasoff duty to warn or protect. Although Tarasoff involved a psychiatrist, this provision is not limited to disclosures by psychiatrists or other mental health professionals. As stated in the preamble of the NPRM, we clarify that § 164.512(j) is not intended to create a duty to warn or disclose protected health information.

Comment: Several comments addressed the portion of proposed § 164.510(k) that would have provided a presumption of reasonable belief to covered entities that disclosed protected health information pursuant to this provision, when such disclosures were made in good faith, based on credible representation by a person with apparent knowledge or authority. Some commenters recommended that this standard be applied to all permissible disclosures without consent or to such disclosures to law enforcement officials.

Alternatively, a group representing health care provider management firms believed that the proposed presumption of reasonable belief would not have provided covered entities with sufficient protection from liability exposure associated with improper uses or disclosures. This commenter recommended that a general good-faith standard apply to covered entities' decisions to disclose protected health information to law enforcement officials. A health plan said that HHS should consider applying the standard of reasonable belief to all uses and disclosures that would have been allowed under proposed § 164.510. Another commenter questioned how the good-faith presumption would apply if the information came from a confidential informant or from a person rather than a doctor, law enforcement official, or government official. (The NPRM listed doctors, law enforcement officials, and other government officials as examples of persons who may make credible representations pursuant to this section.)

Response: As discussed above, this provision is intended to apply in rare circumstances—circumstances that occur much less frequently than those described in other parts of the rule. Due to the importance of averting serious and imminent threats to health and safety, we believe it is appropriate to apply a presumption of good faith to covered entities disclosing protected health information under this section. We believe that the extremely time-sensitive and urgent conditions surrounding the need to avert a serious and imminent threat to the health or safety are fundamentally different from those involved in disclosures that may be made pursuant to other sections of the rule. Therefore, we do not believe it would be appropriate to apply to other sections of the rule the presumption of good faith that applies in § 164.512(j). We clarify that we intend for the presumption of good faith to apply if the disclosure is made in good faith based upon a credible representation by any person with apparent knowledge or authority—not just by doctors, law enforcement or other government officials. Our listing of these persons in the NPRM was illustrative only, and it was not intended to limit the types of

persons who could make such a credible representation to a covered entity.

Comment: One commenter questioned under what circumstances proposed § 164.510(k) would apply instead of proposed § 164.510(f)(5), ''Urgent Circumstances,'' which permitted covered entities to disclose protected health information to law enforcement officials about individuals who are or are suspected to be victims of a crime, abuse, or other harm, if the law enforcement official represents that the information is needed to determine whether a violation of law by a person other than the victim has occurred and immediate law enforcement activity that depends upon obtaining such information may be necessary.

Response: First, we note that inclusion of this provision as § 164.510(f)(5) was a drafting error which subsequently was clarified in technical corrections to the NPRM. In fact, proposed § 164.510(f)(3) addressed the identical circumstances, which in this subsection were titled ''Information about a Victim of Crime or Abuse.'' The scenarios described under § 164.510(f)(3) may or may not involve serious and imminent threats to health or safety.

Second, as discussed in the main section of the preamble to § 164.512(j), we recognize that in some situations, more than one section of this rule potentially could apply with respect to a covered entity's potential disclosure of protected health information. We clarify that if a situation fits one section of the rule (*e.g.,* § 164.512(j) on serious and imminent threats to health or safety), health plans and covered health care providers may disclose protected health information pursuant to that section, regardless of whether the disclosure also could be made pursuant to another section (*e.g.,* §§ 164.512(f)(2) or 164.512(f)(3), regarding disclosure of protected health information about suspects or victims to law enforcement officials), except as otherwise stated in the rule.

Comment: A state health department indicated that the disclosures permitted under this section may be seen as conflicting with existing law in many states.

Response: As indicated in the regulation text for § 164.512(j), this section allows disclosure consistent with applicable law and standards of ethical conduct. We do not preempt any state law that would prohibit disclosure of protected health information in the circumstances to which this section applies. (See Part 160, Subpart B.)

Comment: Many commenters stated that the rule should require that any disclosures should not modify ''duty to warn'' case law or statutes.

Response: The rule does not affect case law or statutes regarding ''duty to warn.'' In § 164.512(j), we specifically permit covered entities to disclose protected health information without authorization for the purpose of protecting individuals from imminent threats to health and safety, consistent with state laws and ethical obligations.

Section 164.512(k)—Uses and Disclosures for Specialized Government Functions

Military Purposes

Armed Forces Personnel and Veterans

Comment: A few comments opposed the proposed rule's provisions on the military, believing that they were too broad. Although acknowledging that the Armed Forces may have legitimate needs for access to protected health data, the commenters believed that the rule failed to provide adequate procedural protections to individuals. A few comments said that, except in limited circumstances or emergencies, covered entities should be required to obtain authorization before using or disclosing protected health information. A few comments also expressed concern over the proposed rule's lack of specific safeguards to protect the health information of victims of domestic violence and abuse. While the commenters said they understood why the military needed access to health information, they did not believe the rule would impede such access by providing safeguards for victims of domestic violence or abuse.

Response: We note that the military comprises a unique society and that members of the Armed Forces do not have the same freedoms as do civilians. The Supreme Court held in *Goldman* v. *Weinberger,* 475 US 503 (1986), that the military must be able to command its members to sacrifice a great many freedoms enjoyed by civilians and to endure certain limits on the freedoms they do enjoy. The Supreme Court also held in *Parker* v. *Levy,* 417 US 733 (1974), that the different character of the military community and its mission required a different application of Constitutional protections. What is permissible in the civilian world may be impermissible in the military. We also note that individuals entering military service are aware that they will not have, and enjoy, the same rights as others.

The proposed rule would have authorized covered entities to use and disclose protected health information about armed forces personnel only for activities considered necessary by appropriate military command authorities to assure the proper execution of the military mission. In order for the military mission to be achieved and maintained, military command authorities need protected health information to make determinations regarding individuals' medical fitness to perform assigned military duties.

The proposed rule required the Department of Defense (DoD) to publish a notice in the **Federal Register** identifying its intended uses and disclosures of protected health information, and we have retained this approach in the final rule. This notice will serve to limit command authorities' access to protected health information to circumstances in which disclosure of protected health information is necessary to assure proper execution of the military mission.

With respect to comments regarding the lack of procedural safeguards for individuals, including those who are victims of domestic violence and abuse, we note that the rule does not provide new authority for covered entities providing health care to individuals who are Armed Forces personnel to use and disclose protected health information. Rather, the rule allows the Armed Forces to use and disclose such information only for those military mission purposes which will be published separately in the **Federal Register**. In addition, we note that the Privacy Act of 1974, as implemented by the DoD, provides numerous protections to individuals.

We modify the proposal to publish privacy rules for the military in the **Federal Register**. The NPRM would have required this notice to include information on the activities for which use or disclosure of protected health information would occur in order to assure proper execution of the military mission. We believe that this proposed portion of the notice is redundant and thus unnecessary in light the rule's application to military services. In the final rule, we eliminate this proposed section of the notice, and we state that health plans and covered health care providers may use and disclose protected health information of Armed Forces personnel for activities considered necessary by appropriate military command authorities to assure the proper execution of a military mission, where the appropriate military authority has published a **Federal Register** notice identifying: (1) The appropriate military command authorities; and (2) the purposes for

which protected health information may be used or disclosed.

Comment: A few commenters, members of the affected beneficiary class, which numbers approximately 2.6 million (active duty and reserve military personnel), opposed proposed § 164.510(m) because it would have allowed a non-governmental covered entity to provide protected health information without authorization to the military. These commenters were concerned that military officials could use the information as the basis for taking action against individuals.

Response: The Secretary does not have the authority under HIPAA to regulate the military's re-use or re-disclosure of protected health information obtained from health plans and covered health care providers. This provision's primary intent is to ensure that proper military command authorities can obtain needed medical information held by covered entities so that they can make appropriate determinations regarding the individual's medical fitness or suitability for military service. Determination that an individual is not medically qualified for military service would lead to his or her discharge from or rejection for service in the military. Such actions are necessary in order for the Armed Forces to have medically qualified personnel, ready to perform assigned duties. Medically unqualified personnel not only jeopardize the possible success of a mission, but also pose an unacceptable risk or danger to others. We have allowed such uses and disclosures for military activities because it is in the Nation's interest.

Separation or Discharge from Military Service

Comment: The preamble to the NPRM solicited comments on the proposal to permit the DoD to transfer, without authorization, a service member's military medical record to the Department of Veterans Affairs (DVA) when the individual completed his or her term of military service. A few commenters opposed the proposal, believing that authorization should be obtained. Both the DoD and the DVA supported the proposal, noting that transfer allows the DVA to make timely determinations as to whether a veteran is eligible for benefits under programs administered by the DVA.

Response: We note that the transfer program was established based on recommendations by Congress, veterans groups, and veterans; that it has existed for many years; and that there has been no objection to, or problems associated with, the program. We also note that the Department of Transportation (DoT) and the Department of Veterans Affairs operate an analogous transfer program with respect to United States Coast Guard personnel, who comprise part of the U.S. Armed Forces. The protected health information involved the DoD/DVA transfer program is being disclosed and used for a limited purpose that directly benefits the individual. This information is covered by, and thus subject to the protections of, the Privacy Act. For these reasons, the final rule retains the DoD/DVA transfer program proposed in the NPRM. In addition, we expand the NPRM's proposed provisions regarding the Department of Veterans Affairs to include the DoT/DVA program, to authorize the continued transfer of these records.

Comment: The Department of Veterans Affairs supported the NPRM's proposal to allow it to use and disclose protected health information among components of the Department so that it could make determinations on whether an individual was entitled to benefits under laws administered by the Department. Some commenters said that the permissible disclosure pursuant to this section appeared to be sufficiently narrow in scope, to respond to an apparent need. Some commenters also said that the DVA's ability to make benefit determinations would be hampered if an individual declined to authorize release of his or her protected health information. A few commenters, however, questioned whether such an exchange of information currently occurs between the components. A few commenters also believed the proposed rule should be expanded to permit sharing of information with other agencies that administer benefit programs.

Response: The final rule retains the NPRM's approach regarding use and disclosure of protected health information without authorization among components of the DVA for the purpose of making eligibility determinations based on commenters' assessment that the provision was narrow in scope and that an alternative approach could negatively affect benefit determinations for veterans. We modify the NPRM language slightly, to clarify that it refers to a health plan or covered health care provider that is a component of the DVA. These component entities may use or disclose protected health information without authorization among various components of the Department to determine eligibility for or entitlement to veterans' benefits. The final rule does not expand the scope of permissible disclosures under this provision to allow the DVA to share such information with other agencies. Other agencies may obtain this information only with authorization, subject to the requirements of § 164.508.

Foreign Military Personnel

Comments: A few comments opposed the exclusion of foreign diplomatic and military personnel from coverage under the rule. These commenters said that the mechanisms that would be necessary to identify these personnel for the purpose of exempting them from the rule's standards would create significant administrative difficulties. In addition, they believed that this provision would have prohibited covered entities from making disclosures allowed under the rule. Some commenters were concerned that implementation of the proposed provision would result in disparate treatment of foreign military and diplomatic personnel with regard to other laws, and that it would allow exploitation of these individuals' health information. These commenters believed that the proposed rule's exclusion of foreign military and diplomatic personnel was unnecessarily broad and that it should be narrowed to meet a perceived need. Finally, they noted that the proposed exclusion could be affected by the European Union's Data Protection Directive.

Response: We agree with the commenters' statement that the NPRM's exclusion of foreign military and diplomatic personnel from the rule's provisions was overly broad. Thus, the final rule's protections apply to these personnel. The rule covers foreign military personnel under the same provisions that apply to all other members of the U.S. Armed Forces, as described above. Foreign military authorities need access to protected health information for the same reason as must United States military authorities: to ensure that members of the armed services are medically qualified to perform their assigned duties. Under the final rule, foreign diplomatic personnel have the same protections as other individuals.

Intelligence Community

Comments: A few commenters opposed the NPRM's provisions regarding protected health information of intelligence community employees and their dependents being considered for postings overseas, on the grounds that the scope of permissible disclosure without authorization was too broad. While acknowledging that the intelligence community may have legitimate needs for its employees' protected health information, the commenters believed that the NPRM

failed to provide adequate procedural protections for the employees' information. A few comments also said that the intelligence community should be able to obtain their employees' health information only with authorization. In addition, commenters said that the intelligence community should make disclosure of protected health information a condition of employment.

Response: Again, we agree that the NPRM's provision allowing disclosure of the protected health information of intelligence community employees without authorization was overly broad. Thus we eliminate it in the final rule. The intelligence community can obtain this information with authorization (pursuant to § 164.508), for example, when employees or their family members are being considered for an oversees assignment and when individuals are applying for employment with or seeking a contract from an intelligence community agency.

National Security and Intelligence Activities and Protective Services for the President and Others

Comment: A number of comments opposed the proposed ''intelligence and national security activities'' provision of the law enforcement section (§ 164.510(f)(4)), suggesting that it was overly broad. These commenters were concerned that the provision lacked sufficient procedural safeguards to prevent abuse of protected health information. The Central Intelligence Agency (CIA) and the Department of Defense (DoD) also expressed concern over the provision's scope. The agencies said that if implemented as written, the provision would have failed to accomplish fully its intended purpose of allowing the disclosure of protected health information to officials carrying out intelligence and national security activities other than law enforcement activities. The CIA and DoD believed that the provision should be moved to another section of the rule, possibly to proposed § 164.510(m) on specialized classes, so that authorized intelligence and national security officials could obtain individuals' protected health information without authorization when lawfully engaged in intelligence and national security activities.

Response: In the final rule, we clarify that this provision does not provide new authority for intelligence and national security officials to acquire health information that they otherwise would not be able to obtain. Furthermore, the rule does not confer new authority for intelligence, national security, or Presidential protective service activities. Rather, the activities permissible under this section are limited to those authorized under current law and regulation (e.g., for intelligence activities, 50 U.S.C. 401, *et seq.*, Executive Order 12333, and agency implementing regulatory authorities). For example, the provision regarding national security activities pertains only to foreign persons that are the subjects of legitimate and lawful intelligence, counterintelligence, or other national security activities. In addition, the provision regarding protective services pertains only to those persons who are the subjects of legitimate investigations for threatening or otherwise exhibiting an inappropriate direction of interest toward U.S. Secret Service protectees pursuant to 18 U.S.C. 871, 879, and 3056. Finally, the rule leaves intact the existing State Department regulations that strictly limit the disclosure of health information pertaining to employees (e.g., Privacy Issuances at State-24 Medical Records).

We believe that because intelligence/national security activities and Presidential/other protective service activities are discrete functions serving different purposes, they should be treated consistently but separately under the rule. For example, medical information is used as a complement to other investigative data that are pertinent to conducting comprehensive threat assessment and risk prevention activities pursuant to 18 U.S.C. 3056. In addition, information on the health of world leaders is important for the provision of protective services and other functions. Thus, § 164.512(k) of the final rule includes separate subsections for national security/intelligence activities and for disclosures related to protective services to the President and others.

We note that the rule does not require or compel a health plan or covered health care provider to disclose protected health information. Rather, two subsections of § 164.512(k) allow covered entities to disclose information for intelligence and national security activities and for protective services to the President and others only to authorized federal officials conducting these activities, when such officials are performing functions authorized by law.

We agree with DoD and CIA that the NPRM, by including these provisions in the law enforcement section (proposed § 164.510(f)), would have allowed covered entities to disclose protected health information for national security, intelligence, and Presidential protective activities only to law enforcement officials. We recognize that many officials authorized by law to carry out intelligence, national security, and Presidential protective functions are not law enforcement officials. Therefore, the final rule allows covered entities to disclose protected health information pursuant to this provision not only to law enforcement officials, but to all federal officials authorized by law to carry out the relevant activities. In addition, we remove this provision from the law enforcement section and include it in § 164.512(k) on uses and disclosures for specialized government functions

Medical Suitability Determinations

Comment: A few comments opposed the NPRM's provision allowing the Department of State to use protected health information for medical clearance determinations. These commenters believed that the scope of permissible disclosures under the proposed provision was too broad. While acknowledging that the Department may have legitimate needs for access to protected health data, the commenters believed that implementation of the proposed provision would not have provided adequate procedural safeguards for the affected State Department employees. A few comments said that the State Department should be able to obtain protected health information for medical clearance determinations only with authorization. A few comments also said that the Department should be able to disclose such information only when required for national security purposes. Some commenters believed that the State Department should be subject to the **Federal Register** notice requirement that the NPRM would have applied to the Department of Defense. A few comments also opposed the proposed provision on the basis that it would conflict with the Rehabilitation Act of 1973 or that it appeared to represent an invitation to discriminate against individuals with mental disorders.

Response: We agree with commenters who believed that the NPRM's provision regarding the State Department's use of protected health information without authorization was unnecessarily broad. Therefore, in the final rule, we restrict significantly the scope of protected health information that the State Department may use and disclose without authorization. First, we allow health plans and covered health care providers that are a component of the State Department to use and disclose protected health information without authorization when making medical suitability determinations for security clearance purposes. For the purposes of a security investigation, these

components may disclose to authorized State Department officials whether or not the individual was determined to be medically suitable. Furthermore, we note that the rule does not confer authority on the Department to disclose such information that it did not previously possess. The Department remains subject to applicable law regarding such disclosures, including the Rehabilitation Act of 1973.

The preamble to the NPRM solicited comment on whether there was a need to add national security determinations under Executive Order 10450 to the rule's provision on State Department uses and disclosures of protected health information for security determinations. While we did not receive comment on this issue, we believe that a limited addition is warranted and appropriate. Executive Orders 10450 and 12968 direct Executive branch agencies to make certain determinations regarding whether their employees' access to classified information is consistent with the national security interests of the United States. Specifically, the Executive Orders state that access to classified information shall be granted only to those individuals whose personal and professional history affirmatively indicates, *inter alia,* strength of character, trustworthiness, reliability, and sound judgment. In reviewing the personal history of an individual, Executive branch agencies may investigate and consider any matter, including a mental health issue or other medical condition, that relates directly to any of the enumerated factors.

In the vast majority of cases, Executive agencies require their security clearance investigators to obtain the individual's express consent in the form of a medical release, pursuant to which the agency can conduct its background investigation and obtain any necessary health information. This rule does not interfere with agencies' ability to require medical releases for purposes of security clearances under these Executive Orders.

In the case of the Department of State, however, it may be impracticable or infeasible to obtain an employee's authorization when exigent circumstances arise overseas. For example, when a Foreign Service Officer is serving at an overseas post and he or she develops a critical medical problem which may or may not require a medical evacuation or other equally severe response, the Department's medical staff have access to the employee's medical records for the purpose of making a medical suitability determination under Executive Orders 10450 and 12968. To restrict the Department's access to information at such a crucial time due to a lack of employee authorization leaves the Department no option but to suspend the employee's security clearance. This action automatically would result in an immediate forced departure from post, which negatively would affect both the Department, due to the unexpected loss of personnel, and the individual, due to the fact that a forced departure can have a long-term impact on his or her career in the Foreign Service.

For this reason, the rule contains a limited security clearance exemption for the Department of State. The exemption allows the Department's own medical staff to continue to have access to an employee's medical file for the purpose of making a medical suitability determination for security purposes. The medical staff can convey a simple ''yes'' or ''no'' response to those individuals conducting the security investigation within the Department. In this way, the Department is able to make security determinations in exigent circumstances without disclosing any specific medical information to any employees other than the medical personnel who otherwise have routine access to these same medical records in an everyday non-security context.

Second, and similarly, the final rule establishes a similar system for disclosures of protected health information necessary to determine worldwide availability or availability for mandatory service abroad under sections 101(a)(4) and 504 of the Foreign Service Act. The Act requires that Foreign Service members be suitable for posting throughout the world and for certain specific assignments. For this reason, we permit a limited exemption to serve the purposes of the statute. Again, the medical staff can convey availability determinations to State Department officials who need to know if certain Foreign Service members are available to serve at post.

Third, and finally, the final rule recognizes the special statutory obligations that the State Department has regarding family members of Foreign Service members under sections 101(b)(5) and 904 of the Foreign Service Act. Section 101(b)(5) of the Foreign Service Act requires the Department of State to mitigate the impact of hardships, disruptions, and other unusual conditions on families of Foreign Service Officers. Section 904 requires the Department to establish a health care program to promote and maintain the physical and mental health of Foreign Service member family members. The final rule permits disclosure of protected health information to officials who need protected health information to determine whether a family member can accompany a Foreign Service member abroad.

Given the limited applicability of the rule, we believe it is not necessary for the State Department to publish a notice in the **Federal Register** to identify the purposes for which the information may be used or disclosed. The final rule identifies these purposes, as described above.

Correctional Institutions

Comments about the rule's application to correctional institutions are addressed in § 164.501, under the definition of ''individual.''

Section 164.512(l)—Disclosures for Workers' Compensation

Comment: Several commenters stated that workers' compensation carriers are excepted under the HIPAA definition of group health plan and therefore we have no authority to regulate them in this rule. These commenters suggested clarifying that the provisions of the proposed rule did not apply to certain types of insurance entities, such as workers' compensation carriers, and that such non-covered entities should have full access to protected health information without meeting the requirements of the rule. Other commenters argued that a complete exemption for workers' compensation carriers was inappropriate.

Response: We agree with commenters that the proposed rule did not intend to regulate workers' compensation carriers. In the final rule we have incorporated a provision that clarifies that the term ''health plan'' excludes ''any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits as defined in section 2791(c)(1) of the PHS Act.'' See discussion above under the definition of ''health plan'' in § 164.501.

Comment: Some commenters argued that the privacy rule should defer to other laws that regulate the disclosure of information to employers and workers' compensation carriers. They commented that many states have laws that require sharing of information—without consent—between providers and employers or workers' compensation carriers.

Response: We agree that the privacy rule should permit disclosures necessary for the administration of state and other workers' compensation systems. To assure that workers' compensations systems are not disrupted, we have added a new

provisions to the final rule. The new § 164.512(l) permits covered entities to disclose protected health information as authorized by and to the extent necessary to comply with workers' compensation or other similar programs established by law that provide benefits for work-related injuries or illnesses without regard to fault. We also note that where a state or other law requires a use or disclosure of protected health information under a workers' compensation or similar scheme, the disclosure would be permitted under § 164.512(a).

Comment: Several commenters stated that if workers' compensation carriers are to receive protected health information, they should only receive the minimum necessary as required in § 164.514. The commenters argued that employers and workers' compensation carriers should not have access to the entire medical history or portions of the medical history that have nothing to do with the injury in question. Further, the covered provider and not the employer or carrier should determine minimum necessary since the provider is a covered entity and only covered entities are subject to sanctions for violations of the rule. These commenters stated that the rule should clearly indicate the ability of covered entities to refuse to disclose protected health information if it went beyond the scope of the injury. Workers' compensation carriers, on the other hand, argued that permitting providers to determine the minimum necessary was inappropriate because determining eligibility for benefits is an insurance function, not a medical function. They stated that workers' compensation carriers need access to the full range of information regarding treatment for the injury underlying the claim, the claimants' current condition, and any preexisting conditions that can either mitigate the claim or aggravate the impact of the injury.

Response: Under the final rule, covered entities must comply with the minimum necessary provisions unless the disclosure is required by law. Our review of state workers' compensation laws suggests that many of these laws address the issue of the scope of information that is available to carriers and employers. The rule permits a provider to disclose information that is authorized by such a law to the extent necessary to comply with such law. Where the law is silent, the workers' compensation carrier and covered health care provider will need to discuss what information is necessary for the carrier to administer the claim, and the health care provider may disclose that information. We note that if the workers' compensation insurer has secured an authorization from the individual for the release of protected health information, the covered entity may release the protected health information described in the authorization.

Section 164.514 Requirements for Uses and Disclosures

Section 164.514(a)–(c)—De-identification

General Approach

Comments: The comments on this topic almost unanimously supported the concept of de-identification and efforts to expand its use. Although a few comments suggested deleting one of the proposed methods or the other, most appeared to support the two method approach for entities with differing levels of statistical expertise.

Many of the comments argued that the standard for creation of de-identified information should be whether there is a ''reasonable basis to believe'' that the information has been de-identified. Others suggested that the ''reasonable basis'' standard was too vague.

A few commenters suggested that we consider information to be de-identified if all personal identifiers that directly reveal the identity of the individual or provide a direct means of identifying individuals have been removed, encrypted or replaced with a code. Essentially, this recommendation would require only removal of ''direct'' identifiers (e.g., name, address, and ID numbers) and allow retention of all ''indirect'' identifiers (e.g., zip code and birth date) in ''de-identified'' information. These comments did not suggest a list or further definition of what identifiers should be considered ''direct'' identifiers.

Some commenters suggested that the standard be modified to reflect a single standard that applies to all covered entities in the interest of reducing uncertainty and complexity. According to these comments, the standard for covered entities to meet for de-identification of protected health information should be generally accepted standards in the scientific and statistical community, rather than focusing on a specified list of identifiers that must be removed.

A few commenters believed that no record of information about an individual can be truly de-identified and that all such information should be treated and protected as identifiable because more and more information about individuals is being made available to the public, such as voter registration lists and motor vehicle and driver's license lists, that would enable someone to match (and identify) records that otherwise appear to be not identifiable.

Response: In the final rule, we reformulate the method for de-identification to more explicitly use the statutory standard of ''a reasonable basis to believe that the information can be used to identify the individual''—just as information is ''individually identifiable'' if there is a reasonable basis to believe that it can be used to identify the individual, it is ''de-identified'' if there is no reasonable basis to believe it can be so used. We also define more precisely how the standard should be applied.

We did not accept comments that suggested that we allow only one method of de-identifying information. We find support for both methods in the comments but find no compelling logic for how the competing interests could be met cost-effectively with only one method.

We also disagree with the comments that advocated using a standard which required removing only the direct identifiers. Although such an approach may be more convenient for covered entities, we judged that the resulting information would often remain identifiable, and its dissemination could result in significant violations of privacy. While we encourage covered entities to remove direct identifiers whenever possible as a method of enhancing privacy, we do not believe that the resulting information is sufficiently blinded as to permit its general dissemination without the protections provided by this rule.

We agree with the comments that said that records of information about individuals cannot be truly de-identified, if that means that the probability of attribution to an individual must be absolutely zero. However, the statutory standard does not allow us to take such a position, but envisions a reasonable balance between risk of identification and usefulness of the information.

We disagree with those comments that advocated releasing only truly anonymous information (which has been changed sufficiently so that it no longer represents actual information about real individuals) and those that supported using only sophisticated statistical analysis before allowing uncontrolled disclosures. Although these approaches would provide a marginally higher level of privacy protection, they would preclude many of the laudable and valuable uses discussed in the NPRM (in § 164.506(d)) and would impose too great a burden on

less sophisticated covered entities to be justified by the small decrease in an already small risk of identification.

We conclude that compared to the alternatives advanced by the comments, the approach proposed in the NPRM, as refined and modified below in response to the comments, most closely meets the intent of the statute.

Comments: A few comments complained that the proposed standards were so strict that they would expose covered entities to liability because arguably no information could ever be de-identified.

Response: In the final rule we have modified the mechanisms by which a covered entity may demonstrate that it has complied with the standard in ways that provide greater certainty. In the standard method for de-identification, we have clarified the professional standard to be used, and anticipate issuing further guidance for covered entities to use in applying the standard. In the safe harbor method, we reduced the amount of judgment that a covered entity must apply. We believe that these mechanisms for de-identification are sufficiently well-defined to protect covered entities that follow them from undue liability.

Comments: Several comments suggested that the rule prohibit any linking of de-identified data, regardless of the probability of identification.

Response: Since our methods of de-identification include consideration of how the information might be used in combination with other information, we believe that linking de-identified information does not pose a significantly increased risk of privacy violations. In addition, since our authority extends only to the regulation of individually identifiable health information, we cannot regulate de-identified information because it no longer meets the definition of individually identifiable health information. We also have no authority to regulate entities that might receive and desire to link such information yet that are not covered entities; thus such a prohibition would have little protective effect.

Comments: Several commenters suggested that we create incentives for covered entities to use de-identified information. One commenter suggested that we mandate an assessment to see if de-identified information could be used before the use or disclosure of identified information would be allowed.

Response: We believe that this final rule establishes a reasonable mechanism for the creation of de-identified information and the fact that this de-identified information can be used without having to follow the policies, procedures, and documentation required to use individually identifiable health information should provide an incentive to encourage its use where appropriate. We disagree with the comment suggesting that we require an assessment of whether de-identified information could be used for each use or disclosure. We believe that such a requirement would be too burdensome on covered entities, particularly with respect to internal uses, where entire records are often used by medical and other personnel. For disclosures, we believe that such an assessment would add little to the protection provided by the minimum necessary requirements in this final rule.

Comments: One commenter asked if de-identification was equivalent to destruction of the protected health information (as required under several of the provisions of this final rule).

Response: The process of de-identification creates a new dataset in addition to the source dataset containing the protected health information. This process does not substitute for actual destruction of the source data.

Modifications to the Proposed Standard for De-Identification

Comments: Several commenters called for clarification of proposed language in the NPRM that would have permitted a covered entity to treat information as de-identified, even if specified identifiers were retained, as long as the probability of identifying subject individuals would be very low. Commenters expressed concern that the ''very low'' standard was vague. These comments expressed concern that covered entities would not have a clear and easy way to know when information meets this part of the standard.

Response: We agree with the comments that covered entities may need additional guidance on the types of analyses that they should perform in determining when the probability of re-identification of information is very low. We note that in the final rule, we reformulate the standard somewhat to require that a person with appropriate knowledge and experience apply generally accepted statistical and scientific methods relevant to the task to make a determination that the risk of re-identification is very small. In this context, we do not view the difference between a very low probability and a very small risk to be substantive. After consulting representatives of the federal agencies that routinely de-identify and anonymize information for public release [16] we attempt here to provide some guidance for the method of de-identification.

As requested by some commenters, we include in the final rule a requirement that covered entities (not following the safe harbor approach) apply generally accepted statistical and scientific principles and methods for rendering information not individually identifiable when determining if information is de-identified. Although such guidance will change over time to keep up with technology and the current availability of public information from other sources, as a starting point the Secretary approves the use of the following as guidance to such generally accepted statistical and scientific principles and methods:

(1) Statistical Policy Working Paper 22—Report on Statistical Disclosure Limitation Methodology (*http://www.fcsm.gov/working-papers/wp22.html*) (prepared by the Subcommittee on Disclosure Limitation Methodology, Federal Committee on Statistical Methodology, Office of Management and Budget); and

(2) The Checklist on Disclosure Potential of Proposed Data Releases (*http://www.fcsm.gov/docs/checklist 799.doc*) (prepared by the Confidentiality and Data Access Committee, Federal Committee on Statistical Methodology, Office of Management and Budget).

We agree with commenters that such guidance will need to be updated over time and we will provide such guidance in the future.

According to the Statistical Policy Working Paper 22, the two main sources of disclosure risk for de-identified records about individuals are the existence of records with very unique characteristics (e.g., unusual occupation or very high salary or age) and the existence of external sources of records with matching data elements which can be used to link with the de-identified information and identify individuals (e.g., voter registration records or driver's license records). The risk of disclosure increases as the number of variables common to both types of records increases, as the accuracy or resolution of the data increases, and as the number of external sources increases. As outlined in Statistical Policy Working Paper 22, an expert disclosure analysis would also consider the probability that an individual who is the target of an attempt at re-identification is represented on both

[16] Confidentiality and Data Access Committee, Federal Committee on Statistical Methodology, Office of Management and Budget.

files, the probability that the matching variables are recorded identically on the two types of records, the probability that the target individual is unique in the population for the matching variables, and the degree of confidence that a match would correctly identify a unique person.

Statistical Policy Working Paper 22 also describes many techniques that can be used to reduce the risk of disclosure that should be considered by an expert when de-identifying health information. In addition to removing all direct identifiers, these include the obvious choices based on the above causes of the risk; namely, reducing the number of variables on which a match might be made and limiting the distribution of the records through a ''data use agreement'' or ''restricted access agreement'' in which the recipient agrees to limits on who can use/receive the data. The techniques also include more sophisticated manipulations: recoding variables into fewer categories to provide less precise detail (including rounding of continuous variables); setting top-codes and bottom-codes to limit details for extreme values; disturbing the data by adding noise by swapping certain variables between records, replacing some variables in random records with mathematically imputed values or averages across small random groups of records, or randomly deleting or duplicating a small sample of records; and replacing actual records with synthetic records that preserve certain statistical properties of the original data.

Modifications to the ''Safe Harbor''

Comments: Many commenters argued that stripping all 19 identifiers is unnecessary for purposes of de-identification. They felt that such items as zip code, city (or county), and birth date, for example, do not identify the individual and only such identifiers as name, street address, phone numbers, fax numbers, email, Social Security number, driver's license number, voter registration number, motor vehicle registration, identifiable photographs, finger prints, voice prints, web universal resource locator, and Internet protocol address number need to be removed to reasonably believe that data has been de-identified.

Other commenters felt that removing the full list of identifiers would significantly reduce the usefulness of the data. Many of these comments focused on research and, to a lesser extent, marketing and undefined ''statistical analysis.'' Commenters who represented various industries and research institutions expressed concern that they would not be able to continue current activities such as development of service provider networks, conducting ''analysis'' on behalf of the plan, studying use of medication and medical devices, community studies, marketing and strategic planning, childhood immunization initiatives, patient satisfaction surveys, and solicitation of contributions. The requirements in the NPRM to strip off zip code and date of birth were of particular concern. These commenters stated that their ability to do research and quality analysis with this data would be compromised without access to some level of information about patient age and/or geographic location.

Response: While we understand that removing the specified identifiers may reduce the usefulness of the resulting data to third parties, we remain convinced by the evidence found in the MIT study that we referred to in the preamble to the proposed rule [17] and the analyses discussed below that there remains a significant risk of identification of the subjects of health information from the inclusion of indirect identifiers such as birth date and zip code and that in many cases there will be a reasonable basis to believe that such information remains identifiable. We note that a covered entity not relying on the safe harbor may determine that information from which sufficient other identifiers have been removed but which retains birth date or zip code is not reasonably identifiable. As discussed above, such a determination must be made by a person with appropriate knowledge and expertise applying generally accepted statistical and scientific methods for rendering information not identifiable.

Although we have determined that all of the specified identifiers must be removed before a covered entity meets the safe harbor requirements, we made modifications in the final rule to the specified identifiers on the list to permit some information about age and geographic area to be retained in de-identified information.

For age, we specify that, in most cases, year of birth may be retained, which can be combined with the age of the subject to provide sufficient information about age for most uses. After considering current and evolving practices and consulting with federal experts on this topic, including members of the Confidentiality and Data Access Committee of the Federal Committee on Statistical Methodology, Office of Management and Budget, we concluded that in general, age is sufficiently broad to be allowed in de-identified information, although all dates that might be directly related to the subject of the information must be removed or aggregated to the level of year to prevent deduction of birth dates. Extreme ages—90 and over—must be aggregated further (to a category of 90+, for example) to avoid identification of very old individuals (because they are relatively rare). This reflects the minimum requirement of the current recommendations of the Bureau of the Census.[18] For research or other studies relating to young children or infants, we note that the rule would not prohibit age of an individual from being expressed as an age in months, days, or hours.

For geographic area, we specify that the initial three digits of zip codes may be retained for any three-digit zip code that contains more than 20,000 people as determined by the Bureau of the Census. As discussed more below, there are currently only 18 three-digit zip codes containing fewer than 20,000 people. We note that this number may change when information from the 2000 Decennial Census is analyzed.

In response to concerns expressed in the comments about the need for information on geographic area, we investigated the potential of allowing 5-digit zip codes or 3-digit zip codes to remain in the de-identified information. According to 1990 Census data, the populations in geographical areas delineated by 3-digit zip codes vary a great deal, from a low of 394 to a high of 3,006,997, with an average size of 282,304. There are two 3-digit zip codes containing fewer than 500 people and six 3-digit zip codes containing fewer than 10,000 people each.[19] Of the total of 881 3-digit zip codes, there are 18 with fewer than 20,000 people, 71 with fewer than 50,000 people, and 215 containing fewer than 100,000 population. We also looked at two-digit zip codes (the first 2 digits of the 5-digit zip code) and found that the smallest of the 98 2-digit zip codes contains 188,638 people.

We also investigated the practices of several other federal agencies which are mandated by Congress to release data

[17] Sweeney, L. Guaranteeing Anonymity when Sharing Medical Data, the Datafly System. Masys, D., Ed. Proceedings, American Medical Informatics Association, Nashville, TN: Hanley & Belfus, Inc., 1997:51–55.

[18] The U.S. Census Bureau's Recommendations Concerning the Census 2000 Public Use Microdata Sample (PUMS) Files [http://www.ipums.org/~census2000/2000pums bureau.pdf], Population Division, U.S. Census Bureau, November 3, 2000.

[19] Figures derived from US Census data on 1990 Decennial Census of Population and Housing, Summary Tape File 3B (STF3B). These data are available to the public (for a fee) at http://www.census.gov/mp/www/rom/msrom6af.html.

from national surveys while preserving confidentiality and which have been dealing with these issues for decades. The problems and solutions being used by these agencies are laid out in detail in the Statistical Policy Working Paper 22 cited earlier.

To protect the privacy of individuals providing information to the Bureau of Census, the Bureau has determined that a geographical region must contain at least 100,000 people.[20] This standard has been used by the Bureau of the Census for many years and is supported by simulation studies using Census data.[21] These studies showed that after a certain point, increasing the size of a geographic area does not significantly decrease the percentage of unique records (i.e., those that could be identified if sampled), but that the point of diminishing returns is dependent on the number and type of demographic variables on which matching might occur. For a small number of demographic variables (6), this point was quite low (about 20,000 population), but it rose quickly to about 50,000 for 10 variables and to about 80,000 for 15 variables. The Bureau of the Census releases sets of data to the public that it considers safe from re-identification because it limits geographical areas to those containing at least 100,000 people and limits the number and detail of the demographic variables in the data. At the point of approximately 100,000 population, 7.3% of records were unique (and therefore potentially identifiable) on 6 demographic variables from the 1990 Census Short Form: Age in years (90 categories), race (up to 180 categories), sex (2 categories), relationship to householder (14 categories), Hispanic (2 categories), and tenure (owner vs. renter in 5 categories). Using 6 variables derived from the Long Form data, age (10 categories), race (6 categories), sex (2 categories), marital status (5 categories), occupation (54 categories), and personal income (10 categories), raised the percentage to 9.8%.

We also examined the results of an NCHS simulation study using national survey data[22] to see if some scientific support could be found for a compromise. The study took random samples from populations of different sizes and then compared the samples to the whole population to see how many records were identifiable, that is, matched uniquely to a unique person in the whole population on the basis of 9 demographic variables: Age (85 categories), race (4 categories), gender (2 categories), ethnicity (2 categories), marital status (3 categories), income (3 categories), employment status (2 categories), working class (4 categories), and occupation (42 categories). Even when some of the variables are aggregated or coded, from the perspective of a large statistical agency desiring to release data to the public, the study concluded that a population size of 500,000 was not sufficient to provide a reasonable guarantee that certain individuals could not be identified. About 2.5 % of the sample from the population of 500,000 was uniquely identifiable, regardless of sample size. This percentage rose as the size of the population decreased, to about 14% for a population of 100,000 and to about 25% for a population of 25,000. Eliminating the occupation variable (which is less likely to be found in health data) reduced this percentage significantly to about 0.4 %, 3%, and 10% respectively. These percentages of unique records (and thus the potentials for re-identification) are highly dependent on the number of variables (which must also be available in other databases which are identified to be considered in a disclosure risk analysis), the categorical breakdowns of those variables, and the level of geographic detail included.

With respect to how we might clarify the requirement to achieve a ''low probability'' that information could be identified, the Statistical Policy Working Paper 22 referenced above discusses the attempts of several researchers to define mathematical measures of disclosure risk only to conclude that ''more research into defining a computable measure of risk is necessary.'' When we considered whether we could specify a maximum level of risk of disclosure with some precision (such as a probability or risk of identification of <0.01), we concluded that it is premature to assign mathematical precision to the ''art'' of de-identification.

After evaluating current practices and recognizing the expressed need for some geographic indicators in otherwise de-identified databases, we concluded that permitting geographic identifiers that define populations of greater than 20,000 individuals is an appropriate standard that balances privacy interests against desirable uses of de-identified data. In making this determination, we focused on the studies by the Bureau of Census cited above which seemed to indicate that a population size of 20,000 was an appropriate cut off if there were relatively few (6) demographic variables in the database. Our belief is that, after removing the required identifiers to meet the safe harbor standards, the number of demographic variables retained in the databases will be relatively small, so that it is appropriate to accept a relatively low number as a minimum geographic size.

In applying this provision, covered entities must replace the (currently 18) forbidden 3-digit zip codes with zeros and thus treat them as a single geographic area (with >20,000 population). The list of the forbidden 3-digit zip codes will be maintained as part of the updated Secretarial guidance referred to above. Currently, they are: 022, 036, 059, 102, 203, 555, 556, 692, 821, 823, 830, 831, 878, 879, 884, 893, 987, and 994. This will result in an average 3-digit zip code area population of 287,858 which should result in an average of about 4% unique records using the 6 variables described above from the Census Short Form. Although this level of unique records will be much higher in the smaller geographic areas, the actual risk of identification will be much lower because of the limited availability of comparable data in publically available, identified databases, and will be further reduced by the low probability that someone will expend the resources to try to identify records when the chance of success is so small and uncertain. We think this compromise will meet the current need for an easy method to identify geographic area while providing adequate protection from re-identification. If a greater level of geographical detail is required for a particular use, the information will have to be obtained through another permitted mechanism or be subjected to a specific de-identification determination as described above. We will monitor the availability of identified public data and the concomitant re-identification risks, both theoretical and actual, and adjust this safe harbor in the future as necessary.

As we stated above, we understand that many commenters would prefer a looser standard for determining when information is de-identified, both generally and with respect to the standards for identifying geographic

[20] Statistical Policy Working Paper 22—Report on Statistical Disclosure Limitation Methodology (*http://www.fcsm.gov/working-papers/wp22.html*) (prepared by the Subcommittee on Disclosure Limitation Methodology, Federal Committee on Statistical Methodology, Office of Management and Budget).

[21] The Geographic Component of Disclosure Risk for Microdata. Brian Greenberg and Laura Voshell. Bureau of the Census Statistical Research Division Report: Census/SRD/RR–90–13, October, 1990.

[22] A Simulation Study of the Identifiability of Survey Respondents when their Community of Residence is Known. John Horm, Natonal Center for Health Statistics, 2000.

area. However, because public databases (such as voter records or driver's license records) that include demographic information about a geographically defined population are available, a surprisingly large percentage of records of health information that contain similar demographic information can be identified. Although the number of these databases seems to be increasing, the number of demographic variables within them still appears to be fairly limited. The number of cases of privacy violation from health records which have been identified in this way is small to date. However, the risk of identification increases with decreasing population size, with increasing amounts of demographic information (both in level of detail and number of variables), and with the uniqueness of the combination of such information in the population. That is, an 18-year-old single white male student is not at risk of identification in a database from a large city such as New York. However, if the database were about a small town where most of the inhabitants were older, retired people of a specific minority race or ethnic group, that same person might be unique in that community and easily identified. We believe that the policy that we have articulated reaches the appropriate balance between reasonably protecting privacy and providing a sufficient level of information to make de-identified databases useful.

Comments: Some comments noted that identifiers that accompany photographic images are often needed to interpret the image and that it would be difficult to use the image alone to identify the individual.

Response: We agree that our proposed requirement to remove all photographic images was more than necessary. Many photographs of lesions, for example, which cannot usually be used alone to identify an individual, are included in health records. In this final rule, the only absolute requirement is the removal of full-face photographs, and we depend on the ''catch-all'' of ''any other unique * * * characteristic * * * '' to pick up the unusual case where another type of photographic image might be used to identify an individual.

Comments: A number of commenters felt that the proposed bar for removal had been set too high; that the removal of these 19 identifiers created a difficult standard, since some identifiers may be buried in lengthy text fields.

Response: We understand that some of the identifiers on our list for removal may be buried in text fields, but we see no alternative that protects privacy. In addition, we believe that such unstructured text fields have little or no value in a de-identified information set and would be removed in any case. With time, we expect that such identifiers will be kept out of places where they are hard to locate and expunge.

Comments: Some commenters asserted that this requirement creates a disincentive for covered entities to de-identify data and would compromise the Secretary's desire to see de-identified data used for a multitude of purposes. Others stated that the ''no reason to believe'' test creates an unreasonable burden on covered entities, and would actually chill the release of de-identified information, and set an impossible standard.

Response: We recognize that the proposed standards might have imposed a burden that could have prevented the widespread use of de-identified information. We believe that our modifications to the final rule discussed above will make the process less burdensome and remove some of the disincentive. However, we could not loosen the standards as far as many commenters wanted without seriously jeopardizing the privacy of the subjects of the information. As discussed above, we modify the ''no reason to know'' standard that was part of the safe harbor provision and replace it in the final rule with an ''actual knowledge'' standard. We believe that this change provides additional certainty to covered entities using the safe harbor and should eliminate any chilling effect.

Comments: Although most commenters wanted to see data elements taken off the list, there were a small number of commenters that wanted to see data items added to the list. They believed that it is also necessary to remove clinical trial record numbers, device model serial numbers, and all proper nouns from the records.

Response: In response to these requests, we have slightly revised the list of identifiers that must be removed under the safe harbor provision. Clinical trial record numbers are included in the general category of ''any other unique identifying number, characteristic, or code.'' These record numbers cannot be included with de-identified information because, although the availability of clinical trial numbers may be limited, they are used for other purposes besides de-identification/re-identification, such as identifying clinical trial records, and may be disclosed under certain circumstances. Thus, they do not meet the criteria in the rule for use as a unique record identifier for de-identified records. Device model serial numbers are included in ''any device identifier or serial number'' and must be removed. We considered the request to remove all proper nouns to be very burdensome to implement for very little increase in privacy and likely to be arbitrary in operation, and so it is not included in the final rule.

Re-Identification

Comments: One commenter wanted to know if the rule requires that covered entities retain the ability to re-identify de-identified information.

Response: The rule does not require covered entities to retain the ability to re-identify de-identified information, but it does allow them to retain this ability.

Comments: A few commenters asked us to prohibit anyone from re-identifying de-identified health information.

Response: We do not have the authority to regulate persons other than covered entities, so we cannot affect attempts by entities outside of this rule to re-identify information. Under the rule, we permit the covered entity that created the de-identified information to re-identify it. However, we include a requirement that, when a unique record identifier is included in the de-identified information, such identifier must not be such that someone other than the covered entity could use it to identify the individual (such as when a derivative of the individual's name is used as the unique record identifier).

Section 164.514(d)—Minimum Necessary

Comment: A large number of commenters objected to the application of the proposed ''minimum necessary'' standard for uses and disclosures of protected health information to uses and disclosures for treatment purposes. Some suggested that the final regulation should establish a good faith exception or safe harbor for disclosures made for treatment.

The overwhelming majority of commenters, generally from the medical community, argued that application of the proposed standard would be contrary to sound medical practice, increase medical errors, and lead to an increase in liability. Some likened the standard to a ''gag clause'' in that it limited the exchange of information critical for quality patient care. They found the standard unworkable in daily treatment situations. They argued that this standard would be potentially dangerous in that it could cause practitioners to withhold information that could be essential for later care. Commenters asserted that caregivers need to be able to give and receive a

complete picture of the patient's health to make a diagnosis and develop a treatment plan.

Other commenters noted that the complexity of medicine is such that it is unreasonable to think that anyone will know the exact parameters of the information another caregiver will need for proper diagnosis and treatment or that a plan will need to support quality assurance and improvement activities. They therefore suggested that the minimum necessary standard be applied instead as an administrative requirement.

Providers also emphasized that they already have an ethical duty to limit the sharing of unnecessary medical information, and most already have well-developed guidelines and practice standards in place. Concerns were also voiced that attempts to provide the minimum necessary information in the treatment setting would lead to multiple editions of a record or creation of summaries that turn out to omit crucial information resulting in confusion and error.

Response: In response to these concerns, we substantially revise the minimum necessary requirements. As suggested by certain commenters, we provide, in § 164.502(b), that disclosures of protected health information to or requests by health care providers for treatment are not subject to the minimum necessary standard. We also modify the requirements for uses of protected health information. This final rule requires covered entities to make determinations of minimum necessary use, including use for treatment purposes, based on the role of the person or class of workforce members rather than at the level of specific uses. A covered entity must establish policies and procedures that identify the types of persons who are to have access to designated categories of information and the conditions, if any, of that access. We establish no requirements specific to a particular use of information. Covered entities are responsible for establishing and documenting these policies and procedures. This approach is consistent with the argument of many commenters that guidelines and practice standards are appropriate means for protecting the privacy of patient information.

Comment: Some commenters argued that the standard should be retained in the treatment setting for uses and disclosures pertaining to mental health information. Some of these commenters asserted that other providers do not need to know the mental status of a patient for treatment purposes.

Response: We agree that the standard should be retained for uses of mental health information in the treatment setting. However, we believe that the arguments for excepting disclosures of protected health information for treatment purposes from application of the minimum necessary standard are also persuasive with respect to mental health information. An individual's mental health can interact with proper treatment for other conditions in many ways. Psychoactive medications may have harmful interactions with drugs routinely prescribed for other purposes; an individual's mental health history may help another health care provider understand the individual's ability to abide by a complicated treatment regimen. For these reasons, it is also not reasonable to presume that, in every case, a health care provider will not need to know an individual's mental health status to provide appropriate treatment.

Providers' comments noted existing ethical duties to limit the sharing of unnecessary medical information, and well-developed guidelines and practice standards for this purpose. Under this rule, providers may use these tools to guide their discretion in disclosing health information for treatment.

Comment: Several commenters urged that covered entities should be required to conspicuously label records to show that they are not complete. They argued that absent such labeling, patient care could be compromised.

Response: We believe that the final policy to except disclosures of protected health information for treatment purposes from application of the minimum necessary standard addresses these commenters' concerns.

Comment: Some commenters argued that the audit exception to the minimum necessary requirements needs to be clarified or expanded, because ''audit'' and ''payment'' are essentially the same thing.

Response: We eliminate this exception. The proposed exclusion of disclosures to health plans for audit purposes is replaced with a general requirement that covered entities must limit requests to other covered entities for individually identifiable health information to what is reasonably necessary for the purpose intended.

Comment: Many commenters argued that the proposed standard was unworkable as applied to ''uses'' by a covered entity's employees, because the proposal appeared not to allow providers to create general policy as to the types of records that particular employees may have access to but instead required that each decision be made ''individually,'' which providers interpret as ''case-by-case.'' Commenters argued that the standard with regard to ''uses'' would be impossible to implement and prohibitively expensive, requiring both medical and legal input to each disclosure decision.

Some commenters recommended deletion of the minimum necessary standard with regard to ''uses.'' Other commenters specifically recommended deletion of the requirement that the standard be applied on an individual, case-by-case basis. Rather, they suggested that the covered entity be allowed to establish general policies to meet the requirement. Another commenter similarly urged that the standard not apply to internal disclosures or for internal health care operations such as quality improvement/assurance activities. The commenter recommended that medical groups be allowed to develop their own standards to ensure that these activities are carried out in a manner that best helps the group and its patients.

Other commenters expressed confusion and requested clarification as to how the standard as proposed would actually work in day-to-day operations within an entity.

Response: Commenters' arguments regarding the workability of this standard as proposed were persuasive, and we therefore make significant modification to address these comments and improve the workability of the standard. For all uses and many disclosures, we require covered entities to include in their policies and procedures (see § 164.530), which may be standard protocols, for ''minimum necessary'' uses and disclosures. We require implementation of such policies in lieu of making the ''minimum necessary'' determination for each separate use and disclosure.

For uses, covered entities must implement policies and procedures that restrict access to and use of protected health information based on the specific professional roles of members of the covered entity's workforce. The policies and procedures must identify the persons or classes of persons in the entity's workforce who need access to protected health information to carry out their duties and the category or categories of protected health information to which such persons or classes need access. These role-based access rules must also identify the conditions, as appropriate, that would apply to such access. For example, an institutional health care provider could allow physicians access to all records under the condition that the viewing of medical records of patients not under their care is recorded and reviewed. Other health professionals' access could

be limited to time periods when they are on duty. Information available to staff who are responsible for scheduling surgical procedures could be limited to certain data. In many instances, use of order forms or selective copying of relevant portions of a record may be appropriate policies to meet this requirement.

Routine disclosures also are not subject to individual review; instead, covered entities must implement policies and procedures (which may be standard protocols) to limit the protected health information in routine disclosures to the minimum information reasonably necessary to achieve the purpose of that type of disclosure. For non-routine disclosures, a covered entity must develop reasonable criteria to limit the protected health information disclosed to the minimum necessary to accomplish the purpose for which disclosure is sought, and to implement procedures for review of disclosures on an individual basis.

We modify the proposed standard to require the covered entity to make ''reasonable efforts'' to meet the minimum necessary standard (not ''all'reasonable efforts, as proposed). What is reasonable will vary with the circumstances. When it is practical to use order forms or selective copying of relevant portions of the record, the covered entity is required to do so. Similarly, this flexibility in the standard takes into account the ability of the covered entity to configure its record system to allow selective access to only certain fields, and the practicality of organizing systems to allow this capacity. It might be reasonable for a covered entity with a highly computerized information system to implement a system under which employees with certain functions have access to only limited fields in a patient records, while other employees have access to the complete records. Such a system might not be reasonable for a covered entity with a largely paper records system.

Covered entities' policies and procedures must provide that disclosure of an entire medical record will not be made except pursuant to policies which specifically justify why the entire medical record is needed.

We believe that these modifications significantly improve the workability of this standard. At the same time, we believe that asking covered entities to assess their practices and establish rules for themselves will lead to significant improvements in the privacy of health information. See the preamble for § 164.514 for a more detailed discussion.

Comment: The minimum necessary standard should not be applied to uses and disclosures for payment or health care operations.

Response: Commenter's arguments for exempting these uses and disclosures from the minimum necessary standard were not compelling. We believe that our modifications to application of the minimum necessary standard to internal uses of protected health information, and to routine disclosures, address many of the concerns raised, particularly the concerns about administrative burdens and the concerns about having the information necessary for day-to-day operations. We do not eliminate this standard in part because we also remain concerned that covered entities may be tempted to disclose an entire medical record when only a few items of information are necessary, to avoid the administrative step of extracting the necessary information (or redacting the unnecessary information). We also believe this standard will cause covered entities to assess their privacy practices, give the privacy interests of their patients and enrollees greater attention, and make improvements that might otherwise not have been made. For this reason, the privacy benefits of retaining the minimum necessary standard for these purposes outweigh the burdens involved. We note that the minimum necessary standard is tied to the purpose of the disclosure; thus, providers may disclose protected health information as necessary to obtain payment.

Comment: Other commenters urged us to apply a ''good faith'' provision to all disclosures subject to the minimum necessary standard. Commenters presented a range of options to modify the proposed provisions which, in their view, would have mitigated their liability if they failed to comply with minimum necessary standard.

Response: We believe that the modifications to this standard, described above, substantially address these commenters' concerns. In addition to allowing the covered entity to use standard protocols for routine disclosures, we modify the standard to require a covered entity to make ''reasonable efforts,'' not ''all'' reasonable efforts as proposed, in making the ''minimum necessary'' disclosure.

Comments: Some commenters complained that language in the proposed rule was vague and provided little guidance, and should be abandoned.

Response: In the preamble for § 164.504 and these responses to comments, we provide further guidance on how a covered entity can develop its policies for the minimum necessary use and disclosure of protected health information. We do not abandon this standard for the reasons described above. We remain concerned about the number of persons who have access to identifiable health information, and believe that causing covered entities to examine their practices will have significant privacy benefits.

Comment: Some commenters asked that the minimum necessary standard should not be applied to disclosures to business partners. Many of these commenters articulated the burdens they would bear if every disclosure to a business partner was required to meet the minimum necessary standard.

Response: We do not agree. In this final rule, we minimize the burden on covered entities in the following ways: in circumstances where disclosures are made on a routine, recurring basis, such as in on-going relationships between covered entities and their business associates, individual review of each routine disclosure has been eliminated; covered entities are required only to develop standard protocols to apply to such routine disclosures made to business associates (or types of business associates). In addition, we allow covered entities to rely on the representation of a professional hired to provide professional services as to what information is the minimum necessary for that purpose.

Comment: Some commenters were concerned that applying the standard in research settings will result in providers declining to participate in research protocols.

Response: We have modified the proposal to reduce the burden on covered entities that wish to disclose protected health information for research purposes. The final rule requires covered entities to obtain documentation or statements from persons requesting protected health information for research that, among other things, describe the information necessary for the research. We allow covered entities to reasonably rely on the documentation or statements as describing the minimum necessary disclosure.

Comment: Some commenters argued that government requests should not be subject to the minimum necessary standard, whether or not they are ''authorized by law.''

Response: We found no compelling reason to exempt government requests from this standard, other than when a disclosure is required by law. (See preamble to § 164.512(a) for the

rationale behind this policy). When a disclosure is required by law, the minimum necessary standard does not apply, whether the recipient of the information is a government official or a private individual.

At the same time, we understand that when certain government officials make requests for protected health information, some covered entities might feel pressure to comply that might not be present when the request is from a private individuals. For this reason, we allow (but do not require) covered entities to reasonably rely on the representations of public officials as to the minimum necessary information for the purpose.

Comment: Some commenters argued that requests under proposed § 164.510 should not be subject to the minimum necessary standard, whether or not they are ''authorized by law.'' Others argued that for disclosures made for administrative proceedings pursuant to proposed § 164.510, the minimum necessary standard should apply unless they are subject to a court order.

Response: We found no compelling reason to exempt disclosures for purposes listed in the regulation from this standard, other than for disclosures required by law. When there is no such legal mandate, the disclosure is voluntary on the part of the covered entity, and it is therefore reasonable to expect the covered entity to make some effort to protect privacy before making such a disclosure. If the covered entity finds that redacting unnecessary information, or extracting the requested information, prior to making the disclosure, is too burdensome, it need not make the disclosure. Where there is ambiguity regarding what information is needed, some effort on the part of the covered entity can be expected in these circumstances.

We also found no compelling reason to limit the exemption for disclosures ''required by law'' to those made pursuant to a court order. The judgment of a state legislature or regulatory body that a disclosure is required is entitled to no less deference than the same decision made by a court. For further rationale for this policy, see the preamble to § 164.512(a).

Comment: Some commenters argued that, in cases where a request for disclosure is not required by law, covered entities should be permitted to rely on the representations by public officials, that they have requested no more than the minimum amount necessary.

Response: We agree, and retain the proposed provision which allows reasonable reliance on the representations of public officials.

Comment: Some commenters argued that it is inappropriate to require covered entities to distinguish between disclosures that are ''required by law'' and those that are merely ''authorized by law,'' for the purposes of determining when the standard applies.

Response: We do not agree. Covered entities have an independent duty to be aware of their legal obligations to federal, state, local and territorial or tribal authorities. In addition, § 164.514(h) allows covered entities to reasonably rely on the oral or written representation of public officials that a disclosure is required by law.

Comment: The minimum necessary standard should not be applied to pharmacists, or to emergency services.

Response: We believe that the final rule's exemption of disclosures of protected health information to health care providers for treatment purposes from the minimum necessary standard addresses these commenters concerns about emergency services. Together with the other changes we make to the proposed standard, we believe we have also addressed most of the commenters' concerns about pharmacists. With respect to pharmacists, the comments offered no persuasive reasons to treat pharmacists differently from other health care providers. Our reasons for retaining this standard for other uses and disclosures of protected health information are explained above.

Comment: A number of commenters argued that the standard should not apply to disclosures to attorneys, because it would interfere with the professional duties and judgment of attorneys in their representation of covered entities. Commenters stated that if a layperson within a covered entity makes an improper decision as to what the minimum necessary information is in regard to a request by the entity's attorney, the attorney may end up lacking information that is vital to representation. These commenters stated that attorneys are usually going to be in a better position to determine what information is truly the minimum necessary for effective counsel and representation of the client.

Response: We found no compelling reason to treat attorneys differently from other business associates. However, to ensure that this rule does not inadvertently cause covered entities to second-guess the professional judgment of the attorneys and other professionals they hire, we modify the proposed policies to explicitly allow covered entities to rely on the representation of a professional hired to provide professional services as to what information is the minimum necessary for that purpose.

Comment: Commenters from the law enforcement community expressed concern that providers may attempt to misuse the minimum necessary standard as a means to restrict access to information, particularly with regard to disclosures for health oversight or to law enforcement officials.

Response: The minimum necessary standard does not apply to disclosures required by law. Since the disclosures to law enforcement officials to which this standard applies are all voluntary, there would be no need for a covered entity to ''manipulate'' the standard; it could decline to make the disclosure.

Comment: Some commenters argued that the only exception to the application of the standard should be when an individual requests access to his or her own information. Many of these commenters expressed specific concerns about victims of domestic violence and other forms of abuse.

Response: We do not agree with the general assertion that disclosure to the individual is the only appropriate exception to the minimum necessary standard. There are other, limited, circumstances in which application of the minimum necessary standard could cause significant harm. For reasons described above, disclosures of protected health information for treatment purposes are not subject to this standard. Similarly, as described in detail in the preamble to § 164.512(a), where another public body has mandated the disclosure of health information, upsetting that judgment in this regulation would not be appropriate.

The more specific concerns expressed about victims of domestic violence and other forms of abuse are addressed in a new provision regarding disclosure of protected health information related to domestic violence and abuse (see § 164.512(c)), and in new limitations on disclosures to persons involved in the individual's care (see § 164.510(b)). We believe that the limitations we place on disclosure of health information in those circumstances address the concerns of these commenters.

Comment: Some commenters argued that disclosures to next of kin should be restricted to minimum necessary protected health information, and to protected health information about only the current medical condition.

Response: In the final regulation, we change the proposed provision regarding ''next of kin'' to more clearly focus on the disclosures we intended to target: Disclosures to persons involved

in the individual's care. We allow such disclosure only with the agreement of the individual, or where the covered entity has offered the individual the opportunity to object to the disclosure and the individual did not object. If the opportunity to object cannot practicably be provided because of the incapacity of the individual or other emergency, we require covered entities to exercise professional judgment in the best interest of the patient in deciding whether to disclose information. In such cases, we permit disclosure only of that information directly relevant to the person's involvement with the individual's health care. (This provision also includes limited disclosure to certain persons seeking to identify or locate an individual.) See § 164.510(b).

Some additional concerns expressed about victims of domestic violence and other forms of abuse are also addressed in a new section on disclosure of protected health information related to domestic violence and abuse. See § 164.512(c). We believe that the limitations we place on disclosure of health information in these provisions address the concerns of these commenters.

Comment: Some commenters argued that covered entities should be required to determine whether de-identified information could be used before disclosing information under the minimum necessary standard.

Response: We believe that requiring covered entities' policies and procedures for minimum necessary disclosures to address whether de-identified information could be used in all instances would impose burdens on some covered entities that could outweigh the benefits of such a requirement. There is significant variation in the sophistication of covered entities' information systems. Some covered entities can reasonably implement policies and procedures that make significant use of de-identified information; other covered entities would find such a requirement excessively burdensome. For this reason, we chose instead to require ''reasonable efforts,'' which can vary according to the situation of each covered entity.

In addition, we believe that the fact that we allow de-identified information to be disclosed without regard to the policies, procedures, and documentation required for disclosure of identifiable health information will provide an incentive to encourage its use where appropriate.

Comment: Several commenters argued that standard transactions should not be subject to the standard.

Response: We agree that data elements that are required or situationally required in the standard transactions should not be, and are not, subject to this standard. However, in many cases, covered entities have significant discretion as to the information included in these transactions. Therefore, this standard does apply to those optional data elements.

Comment: Some commenters asked for clarification to understand how the minimum necessary standard is intended to interact with the security NPRM.

Response: The proposed Security Rule included requirements for electronic health information systems to include access management controls. Under this regulation, the covered entity's privacy policies will determine who has access to what protected health information. We will make every effort to ensure consistency prior to publishing the final Security Rule.

Comment: Many commenters, representing health care providers, argued that if the request was being made by a health plan, the health plan should be required to request only the minimum protected health information necessary. Some of these commenters stated that the requestor is in a better position to know the minimum amount of information needed for their purposes. Some of these commenters argued that the minimum necessary standard should be imposed only on the requesting entity. A few of these commenters argued that both the disclosing and the requesting entity should be subject to the minimum necessary standard, to create ''internal tension'' to assure the standard is honored.

Response: We agree, and in the final rule we require that a request for protected health information made by one covered entity to another covered entity must be limited to the minimum amount necessary for the purpose. As with uses and disclosures of protected health information, covered entities may have standard protocols for routine requests. Similarly, this requirement does not apply to requests made to health care providers for treatment purposes. We modify the rule to balance this provision; that is, it now applies both to disclosure of and requests for protected health information. We also allow, but do not require, the covered entity releasing the information to reasonably rely on the assertion of a requesting covered entity that it is requesting only the minimum protected health information necessary.

Comment: A few commenters suggested that there should be a process for resolving disputes between covered entities over what constitutes the ''minimum necessary'' information.

Response: We do not intend that this rule change the way covered entities currently handle their differences regarding the disclosure of health information. We understand that the scope of information requested from providers by health plans is a source of tension in the industry today, and we believe it would not be appropriate to use this regulation to affect that debate. As discussed above, we require both the requesting and the disclosing covered entity to take privacy concerns into account, but do not inject additional tension into the on-going discussions.

Section 164.514(e)—Marketing

Comment: Many commenters requested clarification of the boundaries between treatment, payment, health care operations, and marketing. Some of these commenters requested clarification of the apparent inconsistency between language in proposed § 164.506(a)(1)(i) (a covered entity is permitted to use or disclose protected health information without authorization ''to carry out'' treatment, payment, or health care operations) and proposed § 164.508(a)(2)(A) (a covered entity must obtain an authorization for all uses and disclosures that are not ''compatible with or directly related to'' treatment, payment, and health care operations). They suggested retaining the language in proposed § 164.508(a)(2)(A), which would permit a broader range of uses and disclosures without authorization, in order to engage in health promotion activities that might otherwise be considered marketing.

Response: In the final rule, we make several changes to the definitions of treatment, payment, and health care operations that are intended to clarify the uses and disclosures of protected health information that may be made for each purpose. See § 164.501 and the corresponding preamble discussion regarding the definitions of these terms. We also have added a definition of the term ''marketing'' to help establish the boundary between marketing and treatment, payment, and health care operations. See § 164.501. We also clarify the conditions under which authorization is or is not required for uses and disclosures of protected health information for marketing purposes. See § 164.514(e). Due to these changes, we believe it is appropriate to retain the wording from proposed § 164.506(a)(1)(i).

Comment: We received a wide variety of suggestions with respect to authorization for uses and disclosures of protected health information for marketing purposes. Some commenters supported requiring authorization for all such uses and disclosures. Other commenters suggested permitting all such uses and disclosures without authorization.

Some commenters suggested we distinguish between marketing to benefit the covered entity and marketing to benefit a third party. For example, a few commenters suggested we should prohibit covered entities from seeking authorization for any use or disclosure for marketing purposes that benefit a third party. These commenters argued that the third parties should be required to obtain the individual's authorization directly from the individual, not through a covered entity, due to the potential for conflicts of interest.

While a few commenters suggested that we require covered entities to obtain authorization to use or disclose protected health information for the purpose of marketing its own products and services, the majority argued these types of marketing activities are vital to covered entities and their customers and should therefore be permitted to occur without authorization. For example, commenters suggested covered entities should be able to use and disclose protected health information without authorization in order to provide appointment reminders, newsletters, information about new initiatives, and program bulletins.

Finally, many commenters argued we should not require authorization for the use or disclosure of protected health information to market any health-related goods and services, even if those goods and services are offered by a third party. Some of these commenters suggested that individuals should have an opportunity to opt out of these types of marketing activities rather than requiring authorization.

Response: We have modified the final rule in ways that address a number of the issues raised in the comments. First, the final rule defines the term marketing, and excepts certain communications from the definition. See § 164.501. These exceptions include communications made by covered entities for the purpose of describing network providers or other available products, services, or benefits and communications made by covered entities for certain treatment-related purposes. These exceptions only apply to oral communications or to written communications for which the covered entity receives no third-party remuneration. The exceptions to the definition of marketing fall within the definitions of treatment and/or health care operations, and therefore uses, or disclosures to a business associate, of protected health information for these purposes are permissible under the rule without authorization.

The final rule also permits covered entities to use protected health information to market health-related products and services, whether they are the products and services of the covered entity or of a third party, subject to a number of limitations. See § 164.514(e). We permit these uses to allow entities in the health sector to inform their patients and enrollees about products that may benefit them. The final rule contains significant restrictions, including requirements that the covered entity disclose itself as the source of a marketing communication, that it disclose any direct or indirect remuneration from third parties for making the disclosure, and that, except in the cases of general communications such as a newsletter, the communication disclose how the individual can opt-out of receiving additional marketing communications. Additional requirements are imposed if the communication is targeted based on the health status or condition of the proposed recipients.

We believe that these modifications address many of the issues raised by commenters and provide a substantial amount of flexibility as to when a covered entity may communicate about a health-related product or service to a patient or enrollee. These communications may include appointment reminders, newsletters, and information about new health products. These changes, however, do not permit a covered entity to disclose protected health information to third parties for marketing (other than to a business associate to make a marketing communication on behalf of the covered entity) without authorization under § 164.508.

Comment: A few commenters suggested we prohibit health care clearinghouses from seeking authorization for the use or disclosure of protected health information for marketing purposes.

Response: We do not prohibit clearinghouses from seeking authorizations for these purposes. We believe, however, that health care clearinghouses will almost always create or obtain protected health information in a business associate capacity. Business associates may only engage in activities involving the use or disclosure of protected health information, including seeking or acting on an authorization, to the extent their contracts allow them to do so. When a clearinghouse creates or receives protected health information other than as a business associate of a covered entity, it is permitted and required to obtain authorizations to the same extent as any other covered entity.

Comment: A few commenters suggested we require covered entities to publicly disclose, on the covered entity's website or upon request, all of their marketing arrangements.

Response: While we agree that such a requirement would provide individuals with additional information about how their information would be used, we do not feel that such a significant intrusion into the business practices of the covered entity is warranted.

Comment: Some commenters argued that if an activity falls within the scope of payment, it should not be considered marketing. Commenters strongly supported an approach which would bar an activity from being construed as ''marketing'' even if performing that activity would result in financial gain to the covered entity. In a similar vein, we were urged to adopt the position that if an activity was considered payment, treatment or health care operations, it could not be further evaluated to determine whether it should be excluded as marketing.

Response: We considered the approach offered by commenters but decided against it. Some activities, such as the marketing of a covered entity's own health-related products or services, are now included in the definition of health care operations, provided certain requirements are met. Other types of activities, such as the sale of a patient list to a marketing firm, would not be permitted under this rule without authorization from the individual. We do not believe that we can envision every possible disclosure of health information that would violate the privacy of an individual, so any list would be incomplete. Therefore, whether or not a particular activity is considered marketing, payment, treatment or health care operations will be a fact-based determination based on the activity's congruence with the particular definition.

Comment: Some industry groups stated that if an activity involves selling products, it is not disease management. They suggested we adopt a definition of disease management that differentiates use of information for the best interests of patient from uses undertaken for ''ulterior purposes'' such as advertising, marketing, or promoting separate products.

Response: We agree in general that the sale of unrelated products to individuals is not a population-based activity that supports treatment and payment. However, in certain circumstances marketing activities are permitted as a health care operation; see the definition of ''health care operations'' in § 164.501 and the related marketing requirements of § 164.514.

Comment: Some commenters complained that the absence of a definition for disease management created uncertainty, in view of the proposed rule's requirement to get authorization for marketing. They expressed concern that the effect would be to require patient consent for many activities that are desirable, not practicably done if authorization is required, and otherwise classifiable as treatment, payment, or health care operations. Examples provided include reminders for appointments, reminders to get preventive services like mammograms, and information about home management of chronic illnesses. They also stated that the proposed rule would prevent many disease management and preventive health activities.

Response: We agree that the distinction in the NPRM between disease management and marketing was unclear. Rather than provide a definition of disease management, this final rule defines marketing. We note that overlap between disease management and marketing exists today in practice and they cannot be distinguished easily with a definitional label. However, for purposes of this rule, the revised language makes clear for what activities an authorization is required. We note that under this rule many of the activities mentioned by commenters will not require authorizations under most circumstances. See the discussion of disease management under the definition of ''treatment'' in § 164.501.

Section 164.514(f)—Fundraising

Comment: Many comments objected to the requirement that an authorization from the individual be obtained for use and disclosure of protected health information for fundraising purposes. They argued that, in the case of not-for-profit health care providers, having to obtain authorization would be time consuming and costly, and that such a requirement would lead to a decrease in charitable giving. The commenters also urged that fundraising be included within the definition of health care operations. Numerous commenters suggested that they did not need unfettered access to patient information in order to carry out their fundraising campaigns. They stated that a limited data set restricted to name, address, and telephone number would be sufficient to meet their needs. Several commenters suggested that we create a voluntary opt-out provision so people can avoid solicitations.

Response: We agree with commenters that our proposal could have adversely effected charitable giving, and accordingly make several modifications to the proposal. First, the final rule allows a covered entity to use or disclose to a business associate protected health information without authorization to identify individuals for fundraising for its own benefit. Permissible fundraising activities include appeals for money, sponsorship of events, etc. They do not include royalties or remittances for the sale of products of third parties (except auctions, rummage sales, etc).

Second, the final rule allows a covered entity to disclose protected health information without authorization to an institutionally related foundation that has as its mission to benefit the covered entity. This special provision is necessary to accommodate tax code provisions which may not allow such foundations to be business associates of their associated covered entity.

We also agree that broad access to protected health information is unnecessary for fundraising and unnecessarily intrudes on individual privacy. The final rule limits protected health information to be used or disclosed for fundraising to demographic information and the date that treatment occurred. Demographic information is not defined in the rule, but will generally include in this context name, address and other contact information, age, gender, and insurance status. The term does not include any information about the illness or treatment.

We also agree that a voluntary opt-out is an appropriate protection, and require in § 164.520 that covered entities provide information on their fundraising activities in their ''Notice of Information Practices.'' As part of the notice and in any fundraising materials, covered entities must provide information explaining how individuals may opt out of fundraising communications.

Comment: Some commenters stated that use and disclosure of protected health information for fundraising, without authorization should be limited to not-for-profit entities. They suggested that not-for-profit entities were in greater need of charitable contributions and as such, they should be exempt from the authorization requirement while for-profit organizations should have to comply with the requirement.

Response: We do not agree that the profit status of a covered entity should determine its allowable use of protected health information for fundraising. Many for-profit entities provide the same services and have similar missions to not-for-profit entities. Therefore, the final rule does not make this distinction.

Comment: Several commenters suggested that the final rule should allow the internal use of protected health information for fundraising, without authorization, but not disclosure for fundraising. These commenters suggested that by limiting access of protected health information to only internal development offices concerns about misuse would be reduced.

Response: We do not agree. A number of commenters noted that they have related charitable foundations that raise funds for the covered entity, and we permit disclosures to such foundations to ensure that this rule does not interfere with charitable giving.

Comment: Several commenters asked us to address the content of fundraising letters. They pointed out that disease or condition-specific letters requesting contributions, if opened by the wrong person, could reveal personal information about the intended recipient.

Response: We agree that such communications raise privacy concerns. In the final rule, we limit the information that can be used or disclosed for fundraising, and exclude information about diagnosis, nature of services, or treatment.

Section 164.514(g)—Verification

Comment: A few commenters suggested that verification guidelines may need to be different as they apply to emergency clinical situations as opposed to routine data collection where delays do not threaten health.

Response: We agree, and make special provisions in §§ 164.510 and 164.512 for disclosures of protected health information by a covered entity without authorization where the individual is unable to agree or object to disclosure due to incapacity or other emergency circumstance.

For example, a health care provider may need to make disclosures to family members, close personal friends, and others involved in the individual's care in emergency situations. Similarly, a health care provider may need to respond to a request from a hospital seeking protected health information in

a circumstance described as an emergency. In each case, we require only that the covered entity exercise professional judgment, in the best interest of the patient, in deciding whether to make a disclosure. Based on the comments and our fact finding, this reflects current practice.

Comment: A few commenters stated the rules should include provisions for electronic verification of identity (such as Public Key Infrastructure (PKI)) as established in the regulations on Security and Electronic Signatures. One commenter suggested that some kind of PKI credentialing certificate should be required.

Response: This regulation does not address specific technical protocols utilized to meet the verification requirements. If the requirements of the rule are otherwise met, the mechanism for meeting them can be determined by the covered entity.

Comment: A few commenters wanted more clarification on the verification procedures. One commenter wanted to know if contract number is enough for verification. A few commenters wanted to know if a callback or authorization on a letterhead is acceptable. A few commenters wanted to know if plans are considered to ''routinely do business'' with all of their members.

Response: In the final rule, we modify the proposed provision and require covered entities to have policies and procedures reasonably designed to verify the identify and authority of persons requesting protected health information. Whether knowledge of a contract number is reasonable evidence of authority and identity will depend on the circumstances. Call-backs and letterhead are typically used today for verification, and are acceptable under this rule if reasonable under the circumstances. For communications with health plan members, the covered entity will already have information about each individual, collected during enrollment, that can be used to establish identity, especially for verbal or electronic inquiries. For example, today many health plans ask for the social security or policy number of individuals seeking information or assistance by telephone. How this verification is done is left up to the covered entity.

Comment: One commenter expressed the need for consistency on verification requirements between this rule and the Security regulation.

Response: We will make every effort to ensure consistency prior to publishing the final Security Rule.

Comment: One commenter stated that the verification language in proposed § 164.518(c)(2)(ii)(B)(1) would have created a presumption that ''a request for disclosure made by official legal process issued by a[n] administrative body'' is reasonable legal authority to disclose the protected health information. The commenter was concerned that this provision could be interpreted to permit a state agency to demand the disclosure of protected health information merely on the basis of a letter signed by an agency representative. The commenter believed that the rule specifically should defer to state or federal law on the disclosure of protected health information pursuant to legal process.

Response: The verification provisions in this rule are minimum requirements that covered entities must meet before disclosing protected health information under this regulation. They do not mandate disclosure, nor do they preempt state laws which impose additional restrictions on disclosure. Where state law regarding disclosures is more stringent, the covered entity must adhere to state law.

Comment: A few commenters wanted the verification requirements to apply to disclosures of protected health information for treatment, payment and operations purposes.

Response: We agree. This verification requirement applies to all disclosures of protected health information permitted by this rule, including for treatment, payment and operations, where the identity of the recipient is not known to the covered entity. Routine communications between providers, where existing relationships have been established, do not require special verification procedures.

Comment: A few commenters were concerned that a verbal inquiry for next of kin verification is not consistent with the verification guidelines of this verification subsection and that verbal inquiry would create problems because anyone who purports to be a next of kin could easily obtain information under false pretenses.

Response: In the final rule in § 164.514, we require the covered entity to verify the identity and authority of persons requesting protected health information, where the identity and authority of such person is not known to the covered entity. This applies to next of kin situations. Procedures for disclosures to next of kin, other family members and persons assisting in an individual's care are also discussed in § 164.510(b), which allows the covered entity to exercise professional judgment as to whether the disclosure is in the individual's best interest when the individual is not available to agree to the disclosure or is incapacitated. Requiring written proof of identity in many of these situations, such as when a family member is seeking to locate a relative in an emergency or disaster situation, would create enormous burden without a corresponding enhancement of privacy, and could cause unnecessary delays in these situations. We therefore believe that reliance on professional judgment provides a better framework for balancing the need for privacy with the need to locate and identify individuals.

Comment: A few commenters stated that the verification requirements will provide great uncertainty to providers who receive authorizations from life, disability income and long-term care insurers in the course of underwriting and claims investigation. They are unaware of any breaches of confidentiality associated with these circumstances and believe the rule creates a solution to a non-existent problem. Another commenter stated that it is too burdensome for health care providers to verify requests that are normally received verbally or via fax.

Response: This rule requires covered health care providers to adhere to current best practices for verification. That is, when the requester is not known to the covered provider, the provider makes a reasonable effort to determine that the protected health information is being sent to the entity authorized to receive it. Our fact finding reveals that this is often done by sending the information to a recognizable organizational address or if being transmitted by fax or phone by calling the requester back through the main organization switchboard rather than through a direct phone number. We agree that these procedures seem to work reasonably well in current practice and are sufficient to meet the relevant requirements in the final rule.

Comments: One comment suggested requiring a form of photo identification such as a driver's license or certain personal information such as date of birth to verify the identity of the individual.

Response: These are exactly the types of standard procedures for verifying the identity of individuals that are envisioned by the final rule. Most health care entities already conduct such procedures successfully. However, it is unwise to prescribe specific means of verification for all situations. Instead, we require policies and procedures reasonably designed for purposes of verification.

Comment: One professional association said that the example procedure described in the NPRM for asking questions to verify that an adult

acting for a young child had the requisite relationship to the child would be quite complex and difficult in practice. The comment asked for specific guidance as to what questions would constitute an adequate attempt to verify such a relationship.

Response: The final rule requires the covered entity to implement policies and procedures that are reasonably designed to comply with the verification requirement in § 164.514. It would not be possible to create the requested specific guidance which could deal with the infinite variety of situations that providers must face, especially the complex ones such as that described by the commenter. As with many of the requirements of this final rule, health care providers are given latitude and expected to make decisions regarding disclosures, based on their professional judgment and experience with common practice, in the best interest of the individual.

Comment: One commenter asserted that ascertaining whether a requestor has the appropriate legal authority is beyond the scope of the training or expertise of most employees in a physician's office. They believe that health care providers must be able to reasonably rely on the authority of the requestor.

Response: In the final regulation we require covered entities to have policies and procedures reasonably designed to verify the identify and authority of persons requesting health information. Where the requester is a public official and legal authority is at issue, we provide detailed descriptions of the acceptable methods for such verification in the final rule. For others, the covered entity must implement policies and procedures that are reasonably designed to comply with the requirement to verify the identity and authority of a requestor, but only if the requestor is unknown to the covered entity. As described above, we expect these policies and procedures to document currently used best practices and reliance on professional judgment in the best interest of the individual.

Comment: One commenter expressed concern that the verification/identification procedures may eliminate or significantly reduce their ability to utilize medical records copy services. As written, they believe the NPRM provides the latitude to set up copy service arrangements, but any change that would add restrictions would adversely affect their ability to process an individual's disability claim.

Response: The covered entity can establish reasonable policies and procedures to address verification in routine disclosures under business associate agreements, with, for example, medical records copy services. Nothing in the verification provisions would preclude those activities, nor have we significantly modified the NPRM provision on this issue.

Section 164.520—Notice of Privacy Practices for Protected Health Information

Comment: Many commenters supported the proposal to require covered entities to produce a notice of information practices. They stated that such notice would improve individuals' understanding of how their information may be used and disclosed and would help to build trust between individuals and covered entities. A few comments, however, argued that the notice requirement would be administratively burdensome and expensive without providing significant benefit to individuals.

Response: We retain the requirement for covered health care providers and health plans to produce a notice of information practices. We additionally require health care clearinghouses that create or receive protected health information other than as a business associate of another covered entity to produce a notice. We believe the notice will provide individuals with a clearer understanding of how their information may be used and disclosed and is essential to inform individuals of their privacy rights. The notice will focus individuals on privacy issues, and prompt individuals to have discussions about privacy issues with their health plans, health care providers, and other persons.

The importance of providing individuals with notice of the uses and disclosures of their information and of their rights with respect to that information is well supported by industry groups, and is recognized in current state and federal law. The July 1977 Report of the Privacy Protection Study Commission recommended that ''each medical-care provider be required to notify an individual on whom it maintains a medical record of the disclosures that may be made of information in the record without the individual's express authorization.'' [23] The Commission also recommended that ''an insurance institution * * * notify (an applicant or principal insured) as to: * * * the types of parties to whom and circumstances under which information about the individual may be disclosed without his authorization, and the types of information that may be disclosed; [and] * * * the procedures whereby the individual may correct, amend, delete, or dispute any resulting record about himself.'' [24] The Privacy Act (5 U.S.C. 552a) requires government agencies to provide notice of the routine uses of information the agency collects and the rights individuals have with respect to that information. In its report ''Best Principles for Health Privacy,'' the Health Privacy Working Group stated, ''Individuals should be given notice about the use and disclosure of their health information and their rights with regard to that information.'' [25] The National Association of Insurance Commissioners' Health Information Privacy Model Act requires carriers to provide a written notice of health information policies, standards, and procedures, including a description of the uses and disclosures prohibited and permitted by the Act, the procedures for authorizing and limiting disclosures and for revoking authorizations, and the procedures for accessing and amending protected health information.

Some states require additional notice. For example, Hawaii requires health care providers and health plans, among others, to produce a notice of confidentiality practices, including a description of the individual's privacy rights and a description of the uses and disclosures of protected health information permitted under state law without the individual's authorization. (HRS section 323C–13)

Today, health plan hand books and evidences of coverage include some of what is required to be in the notice. Industry and standard-setting organizations have also developed notice requirements. The National Committee for Quality Assurance accreditation guidelines state that an accredited managed care organization ''communicates to prospective members its policies and practices regarding the collection, use, and disclosure of medical information [and] * * * informs members * * * of its policies and procedures on * * * allowing members access to their medical records.'' [26] Standards of the American Society for Testing and Materials state,

[23] Privacy Protection Study Commission, ''Personal Privacy in an Information Society,'' July 1977, p. 313.

[24] Privacy Protection Study Commission, ''Personal Privacy in an Information Society,'' July 1977, p. 192.

[25] Health Privacy Working Group, ''Best Principles for Health Privacy,'' Health Privacy Project, Institute for Health Care Research and Policy, Georgetown University, July 1999, p.19.

[26] National Committee on Quality Assurance, ''Surveyor Guidelines for the Accreditation of MCOs,'' effective July 1, 2000—June 30, 2001, p. 324.

''Organizations and individuals who collect, process, handle, or maintain health information should provide individuals and the public with a notice of information practices.'' They recommend that the notice include, among other elements, ''a description of the rights of individuals, including the right to inspect and copy information and the right to seek amendments [and] a description of the types of uses and disclosures that are permitted or required by law without the individual's authorization.'' [27] We build on this well-established principle in this final rule.

Comment: We received many comments on the model notice provided in the proposed rule. Some commenters argued that patients seeing similar documents would be less likely to become disoriented when examining a new notice. Other commenters, however, opposed the inclusion of a model notice or expressed concern about particular language included in the model. They maintained that a uniform model notice would never capture the varying practices of covered entities. Many commenters opposed requirements for a particular format or specific language in the notice. They stated that covered entities should be afforded maximum flexibility in fashioning their notices. Other commenters requested inclusion of specific language as a header to indicate the importance of the notice. A few commenters recommended specific formatting requirements, such as font size or type.

Response: On the whole, we found commenters' arguments for flexibility in the regulation more persuasive than those arguing for more standardization. We agree that a uniform notice would not capture the wide variation in information practices across covered entities. We therefore do not include a model notice in the final rule, and do not require inclusion of specific language in the notice (except for a standard header). We also do not require particular formatting. We do, however, require the notice to be written in plain language. (See above for guidance on writing documents in plain language.) We also agree with commenters that the notice should contain a standard header to draw the individual's attention to the notice and facilitate the individual's ability to recognize the notice across covered entities.

We believe that post-publication guidance will be a more effective mechanism for helping covered entities design their notices than the regulation itself. After the rule is published, we can provide guidance on notice content and format tailored to different types of health plans and providers. We believe such specially designed guidance will be more useful than a one-size-fits-all model notice we might publish with this regulation.

Comment: Commenters suggested that the rule should require that the notice regarding privacy practices include specific provisions related to health information of unemancipated minors.

Response: Although we agree that minors and their parents should be made aware of practices related to confidentiality of protected health information of unemancipated minors, we do not require covered entities that treat minors or use their protected health information to include provisions in their notice that are not required of other covered entities. In general, the content of notice requirements in § 164.520(b) do not vary based on the status of the individual being served. We have decided to maintain consistency by declining to prescribe specific notice requirements for minors. The rule does permit a covered entity to provide individuals with notice of its policies and procedures with respect to anticipated uses and disclosures of protected health information (§ 164.520(b)(2)), and providers are encouraged to do so.

Comment: Some commenters argued that covered entities should not be required to distinguish between those uses and disclosures that are required by law and those that are permitted by law without authorization, because these distinctions may not always be clear and will vary across jurisdictions. Some commenters maintained that simply stating that the covered entity would make all disclosures required by law would be sufficient. Other comments suggested that covered entities should be able to produce very broadly stated notices so that repeated revisions and mailings of those revisions would not be necessary.

Response: While we believe that covered entities have an independent duty to understand the laws to which they are subject, we also recognize that it could be difficult to convey such legal distinctions clearly and concisely in a notice. We therefore eliminate the proposed requirement for covered entities to distinguish between those uses and disclosures that are required by and those that are permitted by law. We instead require that covered entities describe each purpose for which they are permitted or required to use or disclose protected health information under this rule and other applicable law without individual consent or authorization. Specifically, covered entities must describe the types of uses and disclosures they are permitted to make for treatment, payment, and health care operations. They must also describe each of the purposes for which the covered entity is permitted or required by this subpart to use or disclose protected health information without the individual's written consent or authorization (even if they do not plan to make a permissive use or disclosure). We believe this requirement provides individuals with sufficient information to understand how information about them can be used and disclosed and to prompt them to ask for additional information to obtain a clearer understanding, while minimizing covered entities' burden.

A notice that stated only that the covered entity would make all disclosures required by law, as suggested by some of these commenters, would fail to inform individuals of the uses and disclosures of information about them that are permitted, but not required, by law. We clarify that each and every disclosure required by law need not be listed on the notice. Rather, the covered entity can include a general statement that disclosures required by law will be made.

Comment: Some comments argued that the covered entity should not have to provide notice about uses and disclosures that are permitted under the rule without authorization. Other comments suggested that the notice should inform individuals about all of the uses and disclosures that may be made, with or without the individual's authorization.

Response: When the individual's permission is not required for uses and disclosures of information, we believe providing the required notice is the most effective means of ensuring that individuals are aware of how information about them may be shared. The notice need not describe uses and disclosures for which the individual's permission is required, because the individual will be informed of these at the time permission to use or disclose the information is requested.

We additionally require covered entities, even those required to obtain the individual's consent for use and disclosure of protected health information for treatment, payment, and health care operations, to describe those uses and disclosures in their notice. (See § 164.506 and the corresponding preamble discussion regarding consent requirements.) We require these uses

[27] ASTM, ''Standard Guide for Confidentiality, Privacy, Access and Data Security, Principles for Health Information Including Computer-Based Patient Records,'' E 1869–97, § 9.2.

and disclosures to be described in the notice in part in order to reduce the administrative burden on covered providers that are required to obtain consent. Rather than obtaining a new consent each time the covered provider's information policies and procedures are materially revised, covered providers may revise and redistribute their notice. We also expect that the description of how information may be used to carry out treatment, payment, and health care operations in the notice will be more detailed than in the more general consent document.

Comment: Some commenters argued that covered entities should not be required to provide notice of the right to request restrictions, because doing so would be burdensome to the covered entity and distracting to the individual; because individuals have the right whether they are informed of such right or not; and because the requirement would be unlikely to improve patient care.

Response: We disagree. We believe that the ability of an individual to request restrictions is an important privacy right and that informing people of their rights improves their ability to exercise those rights. We do not believe that adding a sentence to the notice is burdensome to covered entities.

Comment: We received comments supporting inclusion of a contact point in the notice, so that individuals will not be forced to make multiple calls to find someone who can assist them with the issues in the notice.

Response: We retain the requirement, but clarify that the title of the contact person is sufficient. A person's name is not required.

Comment: Some commenters argued that we could facilitate compliance by requiring the notice to include the proposed requirement that covered entities use and disclose only the minimum necessary protected health information.

Response: We do not agree that adding such a requirement would strengthen the notice. The purpose of the notice is to inform individuals of their privacy rights, and of the purposes for which protected health information about them may be used or disclosed. Informing individuals that covered entities may use and disclose only the minimum necessary protected health information for a purpose would not increase individuals' understanding of their rights or the purposes for which information may be used or disclosed.

Comment: A few commenters supported allowing covered entities to apply changes in their information practices to protected health information obtained prior to the change. They argued that requiring different protections for information obtained at different times would be inefficient and extremely difficult to administer. Some comments supported requiring covered entities to state in the notice that the information policies and procedures are subject to change.

Response: We agree. In the final rule, we provide a mechanism by which covered entities may revise their privacy practices and apply those revisions to protected health information they already maintain. We permit, but do not require, covered entities to reserve the right to change their practices and apply the revised practices to information previously created or obtained. If a covered entity wishes to reserve this right, it must make a statement to that effect in its notice. If it does not make such a statement, the covered entity may still revise its privacy practices, but it may apply the revised practices only to protected health information created or obtained after the effective date of the notice in which the revised practices are reflected. See § 164.530(i) and the corresponding preamble discussion of requirements regarding changes to information policies and procedures.

Comment: Some commenters requested clarification of the term ''material changes'' so that entities will be comfortable that they act properly after making changes to their information practices. Some comments stated that entities should notify individuals whenever a new category of disclosures to be made without authorization is created.

Response: The concept of ''material change'' appears in other notice laws, such as the ERISA requirements for summary plan descriptions. We therefore retain the ''materiality'' condition for revision of notices, and encourage covered entities to draw on the concept as it has developed through those other laws. We agree that the addition of a new category of use or disclosure of health information that may be made without authorization would likely qualify as a material change.

Comment: We proposed to permit covered entities to implement revised policies and procedures without first revising the notice if a compelling reason existed to do so. Some commenters objected to this proposal because they were concerned that the ''compelling reason'' exception would give covered entities broad discretion to engage in post hoc violations of its own information practices.

Response: We agree and eliminate this provision. Covered entities may not implement revised information policies and procedures before properly documenting the revisions and updating their notice. See § 164.530(i). Because in the final rule we require the notice to include all disclosures that may be made, not only those the covered entity intends to make, we no longer need this provision to accommodate emergencies.

Comment: Some comments suggested that we require covered entities to maintain a log of all past notices, with changes from the previous notice highlighted. They further suggested we require covered entities to post this log on their web sites.

Response: In accordance with § 164.530(j)(2), a covered entity must retain for six years a copy of each notice it issues. We do not require highlighting of changes to the notice or posting of prior notices, due to the associated administrative burdens and the complexity such a requirement would build into the notice over time. We encourage covered entities, however, to make such materials available upon request.

Comment: Several commenters requested clarification about when, relative to the compliance date, covered entities are required to produce their notice. One commenter suggested that covered entities be allowed a period not less than 180 days after adoption of the final rule to develop and distribute the notice. Other comments requested that the notice compliance date be consistent with other HIPAA regulations.

Response: We require covered entities to have a notice available upon request as of the compliance date of this rule (or the compliance date of the covered entity if such date is later). See § 164.534 and the corresponding preamble discussion of the compliance date.

Comment: Some commenters suggested that covered entities, particularly covered health care providers, should be required to discuss the notice with individuals. They argued that posting a notice or otherwise providing the notice in writing may not achieve the goal of informing individuals of how their information will be handled, because some individuals may not be literate or able to function at the reading level used in the notice. Others argued that entities should have the flexibility to choose alternative modes of communicating the information in the notice, including voice disclosure. In contrast, some commenters were concerned that requirements to provide the notice in plain language or in languages other than English would be overly burdensome.

Response: We require covered entities to write the notice in plain language so that the average reader will be able to understand the notice. We encourage, but do not require, covered entities to consider alternative means of communicating with certain populations. We note that any covered entity that is a recipient of federal financial assistance is generally obligated under Title VI of the Civil Rights Act of 1964 to provide material ordinarily distributed to the public in the primary languages of persons with limited English proficiency in the recipients' service areas. While we believe the notice will prompt individuals to initiate discussions with their health plans and health care providers about the use and disclosure of health information, we believe this should be a matter left to each individual and that requiring covered entities to initiate discussions with each individual would be overly burdensome.

Comment: Some commenters suggested that covered entities, particularly health plans, should be permitted to distribute their notice in a newsletter or other communication with individuals.

Response: We agree, so long as the notice is sufficiently separate from other important documents. We therefore prohibit covered entities from combining the notice in a single document with either a consent (§ 164.506) or an authorization (§ 164.508), but do not otherwise prohibit covered entities from including the notice in or with other documents the covered entity shares with individuals.

Comment: Some comments suggested that covered entities should not be required to respond to requests for the notice from the general public. These comments indicated that the requirement would place an undue burden on covered entities without benefitting individuals.

Response: We proposed that the notice be publicly available so that individuals may use the notice to compare covered entities' privacy practices and to select a health plan or health care provider accordingly. We therefore retain the proposed requirement for covered entities to provide the notice to any person who requests a copy, including members of the general public.

Comment: Many commenters argued that the distribution requirements for health plans should be less burdensome. Some suggested requiring distribution upon material revision, but not every three years. Some suggested that health plans should only be required to distribute their notice annually or upon re-enrollment. Some suggested that health plans should only have to distribute their notice upon initial enrollment, not re-enrollment. Other commenters supported the proposed approach.

Response: We agree that the notice distribution requirements for health plans can be less burdensome than in the NPRM while still being effective. In the final rule, we reduce health plans' distribution burden in several ways. First, we require health plans to remind individuals every three years of the availability of the notice and of how to obtain a copy of the notice, rather than requiring the notice to be distributed every three years as proposed. Second, we clarify that health plans only have to distribute the notice to new enrollees on enrollment, not to current members of the health plan upon re-enrollment. Third, we specifically allow all covered entities to distribute the notice electronically in accordance with § 164.520(c)(3).

We retain the requirement for health plans to distribute the notice within 60 days of a material revision. We believe the revised distribution requirements will ensure that individuals are adequately informed of health plans' information practices and any changes to those procedures, without unduly burdening health plans.

Comment: Many commenters argued that health plans should not be required to distribute their notice to every person covered by the plan. They argued that distributing the notice to every family member would be unnecessarily duplicative, costly, and difficult to administer. They suggested that health plans only be required to distribute the notice to the primary participant or to each household with one or more insured individuals.

Response: We agree, and clarify in the final rule that a health plan may satisfy the distribution requirement by providing the notice to the named insured on behalf of the dependents of that named insured. For example, a group health plan may satisfy its notice requirement by providing a single notice to each covered employee of the plan sponsor. We do not require the group health plan to distribute the notice to each covered employee and to each covered dependent of those employees.

Comment: Many comments requested clarification about health plans' ability to distribute the notice via other entities. Some commenters suggested that group health plans should be able to satisfy the distribution requirement by providing copies of the notice to plan sponsors for delivery to employees. Others requested clarification that covered health care providers are only required to distribute their own notice and that health plans should be prohibited from using their affiliated providers to distribute the health plan's notice.

Response: We require health plans to distribute their notice to individuals covered by the health plan. Health plans may elect to hire or otherwise arrange for others, including group health plan sponsors and health care providers affiliated with the health plan, to carry out this distribution. We require covered providers to distribute only their own notices, and neither require nor prohibit health plans and health care providers from devising whatever arrangements they find suitable to meet the requirements of this rule. However, if a covered entity arranges for another person or entity to distribute the covered entity's notice on its behalf and individuals do not receive such notice, the covered entity would be in violation of the rule.

Comment: Some comments stated that covered providers without direct patient contact, such as clinical laboratories, might not have sufficient patient contact information to be able to mail the notice. They suggested we require or allow such providers to form agreements with referring providers or other entities to distribute notices on their behalf or to include their practices in the referring entity's own notice.

Response: We agree with commenters' concerns about the potential administrative and financial burdens of requiring covered providers that have indirect treatment relationships with individuals, such as clinical laboratories, to distribute the notice. Therefore, we require these covered providers to provide the notice only upon request. In addition, these covered providers may elect to reach agreements with other entities distribute their notice on their behalf, or to participate in an organized health care arrangement that produces a joint notice. See § 164.520(d) and the corresponding preamble discussion of joint notice requirements.

Comment: Some commenters requested that covered health care providers be permitted to distribute their notice prior to an individual's initial visit so that patients could review the information in advance of the visit. They suggested that distribution in advance would reduce the amount of time covered health care providers' staff would have to spend explaining the notice to patients in the office. Other comments argued that providers should

distribute their notice to patients at the time the individual visits the provider, because providers lack the administrative infrastructure necessary to develop and distribute mass communications and generally have difficulty identifying active patients.

Response: In the final rule, we clarify that covered providers with direct treatment relationships must provide the notice to patients no later than the first service delivery to the patient after the compliance date. For the reasons identified by these commenters, we do not require covered providers to send their notice to the patient in advance of the patient's visit. We do not prohibit distribution in advance, but only require distribution to the patient as of the time of the visit. We believe this flexibility will allow each covered provider to develop procedures that best meet its and its patients' needs.

Comment: Some comments suggested that covered providers should be required to distribute the notice as of the compliance date. They noted that if the covered provider waited to distribute the notice until first service delivery, it would be possible (pursuant to the rule) for a use or disclosure to be made without the individual's authorization, but before the individual receives the notice.

Response: Because health care providers generally lack the administrative infrastructure necessary to develop and distribute mass communications and generally have difficulty identifying active patients, we do not require covered providers to distribute the notice until the first service delivery after the compliance date. We acknowledge that this policy allows uses and disclosure of health information without individuals' consent or authorization before the individual receives the notice. We require covered entities, including covered providers, to have the notice available upon request as of the compliance date of the rule. Individuals may request a copy of the notice from their provider at any time.

Comment: Many commenters were concerned with the requirement that covered providers post their notice. Some commenters suggested that covered hospital-based providers should be able to satisfy the distribution requirements by posting their notice in multiple locations at the hospital, rather than handing the notice to patients—particularly with respect to distribution after material revisions have been made. Some additionally suggested that these covered providers should have copies of the notice available on site. Some commenters emphasized that the notice must be clear and conspicuous to give individuals meaningful and effective notice of their rights. Other commenters noted that posting the notice will not inform former patients who no longer see the provider.

Response: We clarify in the final rule that the requirement to post a notice does not substitute for the requirement to give individuals a notice or make notices available upon request. Covered providers with direct treatment relationships, including covered hospitals, must give a copy of the notice to the individual as of first service delivery after the compliance date. After giving the individual a copy of the notice as of that first visit, the covered provider has no other obligation to actively distribute the notice. We believe it is unnecessarily burdensome to require covered providers to mail the notice to all current and former patients each time the notice is revised, because unlike health plans, providers may have a difficult time identifying active patients. All individuals, including those who no longer see the covered provider, have the right to receive a copy of the notice on request.

If the covered provider maintains a physical delivery site, it must also post the notice (including revisions to the notice) in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered provider to be able to read the notice. The covered provider must also have the notice available on site for individuals to be able to request and take with them.

Comment: Some comments requested clarification about the distribution requirements for a covered entity that is a health plan and a covered health care provider.

Response: Under § 164.504(g), discussed above, covered entities that conduct multiple types of covered functions, such as the kind of entities described in the above comments, are required to comply with the provisions applicable to a particular type of health care function when acting in that capacity. Thus, in the example described above, the covered entity is required by § 164.504(g) to follow the requirements for health plans with respect to its actions as a health plan and to follow the requirements for health care providers with respect to its actions as a health care provider.

Comment: We received many comments about the ability of covered entities to distribute their notices electronically. Many commenters suggested that we permit covered entities to distribute the notice electronically, either via a web site or e-mail. They argued that covered entities are increasingly using electronic technology to communicate with patients and otherwise administer benefits. They also noted that other regulations permit similar documents, such as ERISA-required summary plan descriptions, to be delivered electronically. Some commenters suggested that electronic distribution should be permitted unless the individual specifically requests a hard copy or lacks electronic access. Some argued that entities should be able to choose a least-cost alternative that allows for periodic changes without excessive mailing costs. A few commenters suggested requiring covered entities to distribute notices electronically.

Response: We clarify in the final rule that covered entities may elect to distribute their notice electronically, provided the individual agrees to receiving the notice electronically and has not withdrawn such agreement. We do not require any particular form of agreement. For example, a covered provider could ask an individual at the time the individual requests a copy of the notice whether she prefers to receive it in hard copy or electronic form. A health plan could ask an individual applying for coverage to provide an e-mail address where the health plan can send the individual information. If the individual provides an e-mail address, the health plan can infer agreement to obtain information electronically.

An individual who has agreed to receive the notice electronically, however, retains the right to request a hard copy of the notice. This right must be described in the notice. In addition, if the covered entity knows that electronic transmission of the notice has failed, the covered entity must produce a hard copy of the notice. We believe this provision allows covered entities flexibility to provide the notice in the form that best meets their needs without compromising individuals' right to adequate notice of covered entities' information practices.

We note that covered entities may also be subject to the Electronic Signatures in Global and National Commerce Act. This rule is not intended to alter covered entities' requirements under that Act.

Comment: Some commenters were concerned that covered providers with ''face-to-face'' patient contact would have a competitive disadvantage against covered internet-based providers, because the face-to-face providers would be required to distribute the notice in hard copy while internet-based providers could satisfy the requirement

by requiring review of the notice on the web site before processing an order. They suggested allowing face-to-face covered providers to satisfy the distribution requirement by asking patients to review the notice posted on site.

Response: We clarify in the final rule that covered health care providers that provide services to individuals over the internet have direct treatment relationships with those individuals. Covered internet-based providers, therefore, must distribute the notice at the first service delivery after the compliance date by automatically and contemporaneously providing the notice electronically in response to the individual's first request for service, provided the individual agrees to receiving the notice electronically.

Even though we require all covered entity web sites to post the entity's notice prominently, we note that such posting is not sufficient to meet the distribution requirements. A covered internet-based provider must send the notice electronically at the individual's first request for service, just as other covered providers with direct treatment relationships must give individuals a copy of the notice as of the first service delivery after the compliance date.

We do not intend to create competitive advantages among covered providers. A web-based and a non-web-based covered provider each have the same alternatives available for distribution of the notice. Both types of covered providers may provide either a paper copy or an electronic copy of the notice.

Comment: We received several comments suggesting that some covered entities should be exempted from the notice requirement or permitted to combine notices with other covered entities. Many comments argued that the notice requirement would be burdensome for hospital-based physicians and result in numerous, duplicative notices that would be meaningless or confusing to patients. Other comments suggested that multiple health plans offered through the same employer should be permitted to produce a single notice.

Response: We retain the requirement for all covered health care providers and health plans to produce a notice of information practices. Health care clearinghouses are required to produce a notice of information practices only to the extent the clearinghouse creates or receives protected health information other than as a business associate of a covered entity. See § 164.500(b)(2). Two other types of covered entities are not required to produce a notice: a correctional institution that is a covered entity and a group health plan that provides benefits only through one or more contracts of insurance with health insurance issuers or HMOs.

We clarify in § 164.504(d), however, that affiliated covered entities under common ownership or control may designate themselves as a single covered entity for purposes of this rule. An affiliated covered entity is only required to produce a single notice.

In addition, covered entities that participate in an organized health care arrangement—which could include hospitals and their associated physicians—may choose to produce a single, joint notice, if certain requirements are met. See § 164.501 and the corresponding preamble discussion of organized health care arrangements.

We clarify that each covered entity included in a joint notice must meet the applicable distribution requirements. If any one of the covered entities, however, provides the notice to a given individual, the distribution requirement with respect to that individual is met for all of the covered entities included in the joint notice. For example, a covered hospital and its attending physicians may elect to produce a joint notice. When an individual is first seen at the hospital, the hospital must provide the individual with a copy of the joint notice. Once the hospital has done so, the notice distribution requirement for all of the attending physicians that provide treatment to the individual at the hospital and that are included in the joint notice is satisfied.

Comment: We solicited and received comments on whether to require covered entities to obtain the individual's signature on the notice. Some commenters suggested that requiring a signature would convey the importance of the notice, would make it more likely that individuals read the notice, and could have some of the same benefits of a consent. They noted that at least one state already requires entities to make a reasonable effort to obtain a signed notice. Other comments noted that the signature would be useful for compliance and risk management purposes because it would document that the individual had received the notice.

The majority of commenters on this topic, however, argued that a signed acknowledgment would be administratively burdensome, inconsistent with the intent of the Administrative Simplification requirements of HIPAA, impossible to achieve for incapacitated individuals, difficult to achieve for covered entities that do not have direct contact with patients, inconsistent with other notice requirements under other laws, misleading to individuals who might interpret their signature as an agreement, inimical to the concept of permitting uses and disclosures without authorization, and an insufficient substitute for authorization.

Response: We agree with the majority of commenters and do not require covered entities to obtain the individual's signed acknowledgment of receipt of the notice. We believe that we satisfied most of the arguments in support of requiring a signature with the new policy requiring covered health care providers with direct treatment relationships to obtain a consent for uses and disclosures of protected health information to carry out treatment, payment, and health care operations. See § 164.506 and the corresponding preamble discussion of consent requirements. We note that this rule does not preempt other applicable laws that require a signed notice and does not prohibit a covered entity from requesting an individual to sign the notice.

Comment: Some commenters supported requiring covered entities to adhere to their privacy practices, as described in their notice. They argued that the notice is meaningless if a covered entity does not actually have to follow the practices contained in its notice. Other commenters were concerned that the rule would prevent a covered entity from using or disclosing protected health information in otherwise lawful and legitimate ways because of an intentional or inadvertent omission from its published notice. Some of these commenters suggested requiring the notice to include a description of some or all disclosures that are required or permitted by law. Some commenters stated that the adherence requirement should be eliminated because it would generally inhibit covered entities' ability to innovate and would be burdensome.

Response: We agree that the value of the notice would be significantly diminished absent a requirement that covered entities adhere to the statements they make in their notices. We therefore retain the requirement for covered entities to adhere to the terms of the notice. See § 164.502(i).

Many of these commenters' concerns regarding a covered entity's inability to use or disclose protected health information due to an intentional or inadvertent omission from the notice are addressed in our revisions to the proposed content requirements for the notice. Rather than require covered entities to describe only those uses and

disclosures they anticipate making, as proposed, we require covered entities to describe all uses and disclosures they are required or permitted to make under the rule without the individual's consent or authorization. We permit a covered entity to provide a statement that it will disclose protected health information that is otherwise required by law, as permitted in § 164.512(a), without requiring them to list all state laws that may require disclosure. Because the notice must describe all legally permissible uses and disclosures, the notice will not generally preclude covered entities from making any uses or disclosures they could otherwise make without individual consent or authorization. This change will also ensure that individuals are aware of all possible uses and disclosures that may occur without their consent or authorization, regardless of the covered entity's current practices.

We encourage covered entities, however, to additionally describe the more limited uses and disclosures they actually anticipate making in order to give individuals a more accurate understanding of how information about them will be shared. We expect that certain covered entities will want to distinguish themselves on the basis of their privacy protections. We note that a covered entity that chooses to exercise this option must clearly state that, at a minimum, the covered entity may make disclosures that are required by law and that are necessary to avert a serious and imminent threat to health or safety.

Section 164.522—Rights To Request Privacy Protection for Protected Health Information

Section 164.522(a)—Right of an Individual To Request Restriction of Uses and Disclosures

Comment: Several commenters supported the language in the NPRM regarding the right to request restrictions. One commenter specifically stated that this is a balanced approach that addresses the needs of the few who would have reason to restrict disclosures without negatively affecting the majority of individuals. At least one commenter explained that if we required consent or authorization for use and disclosure of protected health information for treatment, payment, and health care operations then we must also have a right to request restrictions of such disclosure in order to make the consent meaningful.

Many commenters requested that we delete this provision, claiming it would interfere with patient care, payment, and data integrity. Most of the commenters that presented this position asserted that the framework of giving patients control over the use or disclosure of their information is contrary to good patient care because incomplete medical records may lead to medical errors, misdiagnoses, or inappropriate treatment decisions. Other commenters asserted that covered entities need complete data sets on the populations they serve to effectively conduct research and quality improvement projects and that restrictions would hinder research, skew findings, impede quality improvement, and compromise accreditation and performance measurement.

Response: We acknowledge that widespread restrictions on the use and disclosure of protected health information could result in some difficulties related to payment, research, quality assurance, etc. However, in our efforts to protect the privacy of health information about individuals, we have sought a balance in determining the appropriate level of individual control and the smooth operation of the health care system. In the final rule, we require certain covered providers and permit all covered entities to obtain consent from individuals for use and disclosure of protected health information for treatment, payment, and health care operations (see § 164.506). In order to give individuals some control over their health information for uses and disclosures of protected health information for treatment, payment, and health care operations, we provide individuals with the opportunity to request restrictions of such uses and disclosures.

Because the right to request restrictions encourages discussions about how protected health information may be used and disclosed and about an individual's concerns about such uses and disclosures, it may improve communications between a provider and patient and thereby improve care. According to a 1999 survey on the Confidentiality of Medical Records by the California HealthCare Foundation, one out of every six people engage in behavior to protect themselves from unwanted disclosures of health information, such as lying to providers or avoiding seeking care. This indicates that, without the ability to request restrictions, individuals would have incentives to remain silent about important health information that could have an effect on their health and health care, rather than consulting a health care provider.

Further, this policy is not a dramatic change from the status quo. Today, many state laws restrict disclosures for certain types of health information without patient's authorization. Even if there is no mandated requirement to restrict disclosures of health information, providers may agree to requests for restrictions of disclosures when a patient expresses particular sensitivity and concern for the disclosure of health information.

We agree that there may be instances in which a restriction could negatively affect patient care. Therefore, we include protections against this occurrence. First, the right to request restrictions is a right of individuals to make the request. A covered entity may refuse to restrict uses and disclosures or may agree only to certain aspects of the individual's request if there is concern for the quality of patient care in the future. For example, if a covered provider believes that it is not in the patient's best medical interest to have such a restriction, the provider may discuss the request for restriction with the patient and give the patient the opportunity to explain the concern for disclosure. Also, a covered provider who is concerned about the implications on future treatment can agree to use and disclose sensitive protected health information for treatment purposes only and agree not to disclose information for payment and operation purposes. Second, a covered provider need not comply with a restriction that has been agreed to if the individual who requested the restriction is in need of emergency treatment and the restricted protected health information is needed to provide the emergency treatment. This exception should limit the harm to health that may otherwise result from restricting the use or disclosure of protected health information. We encourage covered providers to discuss with individuals that the information may be used or disclosed in emergencies. We require that the covered entity that discloses restricted protected health information in an emergency request that the health care provider that receives such information not further use or re-disclose the information.

Comment: Some health plans stated that an institutionalized right to restrict can interfere with proper payment and can make it easier for unscrupulous providers or patients to commit fraud on insurance plans. They were concerned that individuals could enter into restrictions with providers to withhold information to insurance companies so that the insurance company would not know about certain conditions when underwriting a policy.

Response: This rule does not enhance the ability of unscrupulous patients or health care providers to engage in deceptive or fraudulent withholding of information. This rule grants a right to request a restriction, not an absolute right to restrict. Individuals can make such requests today. Other laws criminalize insurance fraud; this regulation does not change those laws.

Comment: One commenter asserted that patients cannot anticipate the significance that one aspect of their medical information will have on treatment of other medical conditions, and therefore, allowing them to restrict use or disclosure of some information is contrary to the patient's best interest.

Response: We agree that patients may find it difficult to make such a calculus, and that it is incumbent on health care providers to help them do so. Health care providers may deny requests for or limit the scope of the restriction requested if they believe the restriction is not in the patient's best interest.

Comment: One commenter asked whether an individual's restriction to disclosure of information will be a bar to liability for misdiagnosis or failure to diagnose by a covered entity who can trace its error back to the lack of information resulting from such restriction.

Response: Decisions regarding liability and professional standards are determined by state and other law. This rule does not establish or limit liability for covered entities under those laws. We expect that the individual's request to restrict the disclosure of their protected health information would be considered in the decision of whether or not a covered entity is liable.

Comment: One commenter requested that we allow health plans to deny coverage or reimbursement when a covered health care provider's agreement to restrict use or disclosure prevents the plan from getting the information that is necessary to determine eligibility or coverage.

Response: In this rule, we do not modify insurers' rules regarding information necessary for payment. We recognize that restricting the disclosure of information may result in a denial of payment. We expect covered providers to explain this possibility to individuals when considering their requests for restrictions and to make alternative payment arrangements with individuals if necessary.

Comment: Some commenters discussed the administrative burden and cost of the requirement that individuals have the right to request restrictions and that trying to segregate certain portions of information for protection may be impossible. Others stated that the administrative burden would make providers unable to accommodate restrictions, and would therefore give patients false expectations that their right to request restrictions may be acted upon. One commenter expressed concern that large covered providers would have a particularly difficult time establishing a policy whereby the covered entity could agree to restrictions and would have an even more difficult time implementing the restrictions since records may be kept in multiple locations and accessed by multiple people within the organization. Still other commenters believed that the right to request restrictions would invite argument, delay, and litigation.

Response: We do not believe that this requirement is a significant change from current practice. Providers already respond to requests by patients regarding sensitive information, and are subject to state law requirements not to disclose certain types of information without authorization. This right to request is permissive so that covered entities can balance the needs of particular individuals with the entity's ability to manage specific accommodations.

Comment: Some commenters were concerned that a covered entity would agree to a restriction and then realize later that the information must be disclosed to another caregiver for important medical care purposes.

Response: Some individuals seek treatment only on the condition that information about that treatment will not be shared with others. We believe it is necessary and appropriate, therefore, that when a covered provider agrees to such a restriction, the individual must be able to rely on that promise. We strongly encourage covered providers to consider future treatment implications of agreeing to a restriction. We encourage covered entities to inform others of the existence of a restriction when appropriate, provided that such notice does not amount to a *de facto* disclosure of the restricted information. If the covered provider subject to the restriction believes that disclosing the protected health information that was created or obtained subject to the restriction is necessary to avert harm (and it is not for emergency treatment), the provider must ask the individual for permission to terminate or modify the restriction. If the individual agrees to the termination of the restriction, the provider must document this termination by noting this agreement in the medical record or by obtaining a written agreement of termination from the individual and may use or disclose the information for treatment. If the individual does not agree to terminate or modify the restriction, however, the provider must continue to honor the restriction with respect to protected health information that was created or received subject to the restriction. We note that if the restricted protected health information is needed to provide emergency treatment to the individual who requested the restriction, the covered entity may use or disclose such information for such treatment.

Comment: Commenters asked that we require covered entities to keep an accounting of the requests for restrictions and to report this information to the Department in order for the Department to determine whether covered entities are showing ''good faith'' in dealing with these requests.

Response: We require that covered entities that agree to restrictions with individuals document such restrictions. A covered entity must retain such documentation for six years from the date of its creation or the date when it last was in effect, whichever is later. We do not require covered entities to keep a record of all requests made, including those not agreed to, nor that they report such requests to the Department. The decision to agree to restrictions is that of the covered entity. Because there is no requirement to agree to a restriction, there is no reason to impose the burden to document requests that are denied. Any reporting requirement could undermine the purpose of this provision by causing the sharing, or appearance of sharing, of information for which individuals are seeking extra protection.

Comment: One commenter asserted that providers that currently allow such restrictions will choose not to do so under the rule based on the guidance of legal counsel and loss prevention managers, and suggested that the Secretary promote competition among providers with respect to privacy by developing a third-party ranking mechanism.

Response: We believe that providers will do what is best for their patients, in accordance with their ethics codes, and will continue to find ways to accommodate requested restrictions when they believe that it is in the patients' best interests. We anticipate that providers who find such action to be of commercial benefit will notify consumers of their willingness to be responsive to such requests. Involving third parties could undermine the purpose of this provision, by causing the sharing, or appearance of sharing, of information for which individuals are seeking extra protection.

Comment: One commenter said that any agreement regarding patient-requested restrictions should be in writing before a covered provider would be held to standards for compliance.

Response: We agree that agreed to restrictions must be documented in writing, and we require that covered entities that agree to restrictions document those restrictions in accordance with § 164.530(j). The writing need not be formal; a notation in the medical record will suffice. We disagree with the request that an agreed to restriction be reduced to writing in order to be enforced. If we adopted the requested policy, a covered entity could agree to a restriction with an individual, but avoid being held to this agreed to restriction under the rule by failing to document the restriction. This would give a covered entity the opportunity to agree to a restriction and then, at its sole discretion, determine if it is enforceable by deciding whether or not to make a note of the restriction in the record about the individual. Because the covered entity has the ability to agree or fail to agree to a restriction, we believe that once the restriction is agreed to, the covered entity must honor the agreement. Any other result would be deceptive to the individual and could lead an individual to disclose health information under the assumption that the uses and disclosures will be restricted. Under § 164.522, a covered entity could be found to be in violation of the rule if it fails to put an agreed-upon restriction in writing and also if it uses or discloses protected health information inconsistent with the restriction.

Comment: Some commenters said that the right to request restrictions should be extended to some of the uses and disclosures permitted without authorization in § 164.510 of the NPRM, such as disclosures to next of kin, for judicial and administrative proceedings, for law enforcement, and for governmental health data systems. Other commenters said that these uses and disclosures should be preserved without an opportunity for individuals to opt out.

Response: We have not extended the right to request restrictions under this rule to disclosures permitted in § 164.512 of the final rule. However, we do not preempt other law that would enforce such agreed-upon restrictions. As discussed in more detail, above, we have extended the right to request restrictions to disclosures to persons assisting in the individual's care, such as next of kin, under § 164.510(b). Any restriction that a covered entity agrees to with respect to persons assisting in the individual's care in accordance with the rule will be enforceable under the rule.

Comment: A few commenters raised the question of the effect of a restriction agreed to by one covered entity that is part of a larger covered entity, particularly a hospital. Commenters were also concerned about who may speak on behalf of the covered entity.

Response: All covered entities are required to establish policies and procedures for providing individuals the right to request restrictions, including policies for who may agree to such restrictions on the covered entity's behalf. Hospitals and other large entities that are concerned about employees agreeing to restrictions on behalf of the organization will have to make sure that their policies are communicated appropriately to those employees. The circumstances under which members of a covered entity's workforce can bind the covered entity are a function of other law, not of this regulation.

Comment: Commenters expressed confusion about the intended effect of any agreed-upon restrictions on downstream covered entities. They asserted that it would be extremely difficult for a requested restriction to be followed through the health care system and that it would be unfair to hold covered entities to a restriction when they did not agree to such restriction. Specifically, commenters asked whether a covered provider that receives protected health information in compliance with this rule from a physician or medical group that has agreed to limit certain uses of the information must comply with the original restriction. Other commenters expressed concern that not applying a restriction to downstream covered entities is a loophole and that all downstream covered providers and health plans should be bound by the restrictions.

Response: Under the final rule, a restriction that is agreed to between an individual and a covered entity is only binding on the covered entity that agreed to the restriction and not on downstream entities. It would also be binding on any business associate of the covered entity since a business associate can not use or disclose protected health information in any manner that a covered entity would not be permitted to use or disclose such information. We realize that this may limit the ability of an individual to successfully restrict a use or disclosure under all circumstances, but we take this approach for two reasons. First, we allow covered entities to refuse individuals' requests for restrictions. Requiring downstream covered entities to abide by a restriction would be tantamount to forcing them to agree to a request to which they otherwise may not have agreed. Second, some covered entities have information systems which will allow them to accommodate such requests, while others do not. If the downstream provider is in the latter category, the administrative burden of such a requirement would be unmanageable.

We encourage covered entities to explain this limitation to individuals when they agree to restrictions, so individuals will understand that they need to ask all their health plans and providers for desired restrictions. We also require that a covered entity that discloses protected health information to a health care provider for emergency treatment, in accordance with § 164.522 (a)(iii), to request that the recipient not further use or disclose the information.

Comment: One commenter requested that agreed-to restrictions of a covered entity not be applied to business associates.

Response: As stated in § 164.504(e)(2), business associates are acting on behalf of, or performing services for, the covered entity and may not, with two narrow exceptions, use or disclose protected health information in a manner that would violate this rule if done by the covered entity. Business associates are agents of the covered entity with respect to protected health information they obtain through the business relationship. If the covered entity agrees to a restriction and, therefore, is bound to such restriction, the business associate will also be required to comply with the restriction. If the covered entity has agreed to a restriction, the satisfactory assurances from the business associate, as required in § 164.504(e), must include assurances that protected health information will not be used or disclosed in violation of an agreed to restriction.

Comment: One commenter requested clarification that the right to request restrictions cannot be used to restrict the creation of de-identified information.

Response: We found no reason to treat the use of protected health information to create de-identified information different from other uses of protected health information. The right to request restriction applies to any use or disclosure of protected health information to carry out treatment, payment, or health care operations. If the covered entity uses protected health information to create de-identified information, the covered entity need not agree to a restriction of this use.

Comment: Some commenters stated that individuals should be given a true right to restrict uses and disclosures of protected health information in certain defined circumstances (such as for sensitive information) rather than a right to request restrictions.

Response: We are concerned that a right to restrict could create conflicts with the professional ethical obligations of providers and others. We believe it is better policy to allow covered entities to refuse to honor restrictions that they believe are not appropriate and leave the individual with the option of seeking service from a different covered entity. In addition, many covered entities have information systems that would make it difficult or impossible to accommodate certain restrictions.

Comment: Some commenters requested that self-pay patients have additional rights to restrict protected health information. Others believed that this policy would result in de facto discrimination against those patients that could not afford to pay out-of-pocket.

Response: Under the final rule, the decision whether to tie an agreement to restrict to the way the individual pays for services is left to each covered entity. We have not provided self-pay patients with any special rights under the rule.

Comment: Some commenters suggested that we require restrictions to be clearly noted so that insurers and other providers would be aware that they were not being provided with complete information.

Response: Under the final rule, we do not require or prohibit a covered entity to note the existence of an omission of information. We encourage covered entities to inform others of the existence of a restriction, in accordance with professional practice and ethics, when appropriate to do so. In deciding whether or not to disclose the existence of a restriction, we encourage the covered entity to carefully consider whether disclosing the existence is tantamount to disclosure of the restricted protected health information so as to not violate the agreed to restriction.

Comment: A few commenters said that covered entities should have the right to modify or revoke an agreement to restrict use or disclosure of protected health information.

Response: We agree that, as circumstances change, covered entities should be able to revisit restrictions to which they had previously agreed. At the same time, individuals should be able to rely on agreements to restrict the use or disclosure of information that they believe is particularly sensitive. If a covered entity would like to revoke or modify an agreed-upon restriction, the covered entity must renegotiate the agreement with the individual. If the individual agrees to modify or terminate the restriction, the covered entity must get written agreement from the individual or must document the oral agreement. If the individual does not agree to terminate or modify the restriction, the covered entity must inform the individual that it is modifying or terminating its agreement to the restriction and any modification or termination would apply only with respect to protected health information created or received after the covered entity informed the individual of the termination. Any protected health information created or received during the time between when the restriction was agreed to and when the covered entity informed the individual or such modification or termination remains subject to the restriction.

Comment: Many commenters advocated for stronger rights to request restrictions, particularly that victims of domestic violence should have an absolute right to restrict disclosure of information.

Response: We address restrictions for disclosures in two different ways, the right to request restrictions (§ 164.522(a)) and confidential communications (§ 164.522(b)). We have provided all individuals with a right to request restrictions on uses or disclosures of treatment, payment, and health care operations. This is not an absolute right to restrict. Covered entities are not required to agree to requested restrictions; however, if they do, the rule would require them to act in accordance with the restrictions. (See the preamble regarding § 164.522 for a more comprehensive discussion of the right to request restrictions.)

In the final rule, we create a new provision that provides individuals with a right to confidential communications, in response to these comments. This provision grants individuals with a right to restrict disclosures of information related to communications made by a covered entity to the individual, by allowing the individual to request that such communications be made to the person at an alternative location or by an alternative means. For example, a woman who lives with an abusive man and is concerned that his knowledge of her health care treatment may lead to additional abuse can request that any mail from the provider be sent to a friend's home or that telephone calls by a covered provider be made to her at work. Other reasonable accommodations may be requested as well, such as requesting that a covered provider never contact the individual by a phone, but only contact her by electronic mail. A provider must accommodate an individual's request for confidential communications, under this section, without requiring an explanation as to the reason for the request as a condition of accommodating the request. The individual does not need to be in an abusive situation to make such requests of a covered provider. The only conditions that a covered provider may place on an individual is that the request be reasonable with respect to the administrative burden on the provider, the request to be in writing, the request specify an alternative address or other method of contact, and that (where relevant) the individual provide information about how payment will be handled. What is reasonable may vary by the size or type of covered entity; however, additional modest cost to the provider would not be unreasonable.

An individual also has a right to restrict communications from a health plan. The right is the same as with covered providers except it is limited to cases where the disclosure of information could endanger the individual. A health plan may require an individual to state this fact as a condition of accommodating the individual's request for confidential communications. This would provide victims of domestic violence the right to control such disclosures.

Comment: Commenters opposed the provision of the NPRM (§ 164.506(c)(1)(ii)(B)) stating that an individual's right to request restrictions on use or disclosure of protected health information would not apply in emergency situations as set forth in proposed § 164.510(k). Commenters asserted that victims who have been harmed by violence may first turn to emergency services for help and that, in such situations, the victim should be able to request that the perpetrator not be told of his or her condition or whereabouts.

Response: We agree with some of the commenters' concerns. In the final rule, the right to request restrictions is available to all individuals regardless of the circumstance or the setting in which the individual is obtaining care. For example, an individual that seeks care in an emergency room has the same right to request a restriction as an individual seeking care in the office of a covered physician.

However, we continue to permit a covered entity to disclose protected health information to a health care

provider in an emergency treatment situation if the restricted protected health information is needed to provide the emergency treatment or if the disclosure is necessary to avoid serious and imminent threats to public health and safety. Although we understand the concern of the commenters, we believe that these exceptions are limited and will not cause a covered entity to disclose information to a perpetrator of a crime. We are concerned that a covered provider would be required to delay necessary care if a covered entity had to determine if a restriction exists at the time of such emergency. Even if a covered entity knew that there was a restriction, we permitted this limited exception for emergency situations because, as we had stated in the preamble for § 164.506 of the NPRM, an emergency situation may not provide sufficient opportunity for a patient and health care provider to discuss the potential implications of restricting use and disclosure of protected health information on that emergency. We also believe that the importance of avoiding serious and imminent threats to health and safety and the ethical and legal obligations of covered health care providers' to make disclosures for these purposes is so significant that it is not appropriate to apply the right to request restrictions on such disclosures.

We note that we have included other provisions in the final rule intended to avoid or minimize harm to victims of domestic violence. Specifically, we include provisions in the final rule that allow individuals to opt out of certain types of disclosures and require covered entities to use professional judgment to determine whether disclosure of protected health information is in a patient's best interest (see § 164.510(a) on use and disclosure for facility directories and § 164.510(b) on uses and disclosures for assisting in an individual's care and notification purposes). Although an agreed to restriction under § 164.522 would apply to uses and disclosures for assisting in an individual's care, the opt out provision in § 164.510(b) can be more helpful to a person who is a victim of domestic violence because the individual can opt out of such disclosure without obtaining the agreement of the covered provider. We permit a covered entity to elect not to treat a person as a personal representative (see § 164.502(g)) or to deny access to a personal representative (see § 164.524(a)(3)(iii)) where there are concerns related to abuse. We also include a new § 164.512(c) which recognizes the unique circumstances surrounding disclosure of protected health information about victims of abuse, neglect, and domestic violence.

Section 164.522(b)—Confidential Communications Requirements

Comment: Several commenters requested that we add a new section to prevent disclosure of sensitive health care services to members of the patient's family through communications to the individual's home, such as appointment notices, confirmation or scheduling of appointments, or mailing a bill or explanation of benefits, by requiring covered entities to agree to correspond with the patient in another way. Some commenters stated that this is necessary in order to protect inadvertent disclosure of sensitive information and to protect victims of domestic violence from disclosure to an abuser. A few commenters suggested that a covered entity should be required to obtain an individual's authorization prior to communicating with the individual at the individual's home with respect to health care relating to sensitive subjects such as reproductive health, sexually transmissible diseases, substance abuse or mental health.

Response: We agree with commenters' concerns regarding covered entities' communications with individuals. We created a new provision, § 164.522(b), to address confidential communications by covered entities. This provision gives individuals the right to request that they receive communications from covered entities at an alternative address or by an alternative means, regardless of the nature of the protected health information involved. Covered providers are required to accommodate reasonable requests by individuals and may not require the individual to explain the basis for the request as a condition of accommodation. Health plans are required to accommodate reasonable requests by individuals as well; however, they may require the individual to provide a statement that disclosure of the information could endanger the individual, and they may condition the accommodation on the receipt of such statement.

Under the rule, we have required covered providers to accommodate requests for communications to alternative addresses or by alternative means, regardless of the reason, to limit risk of harm. Providers have more frequent one-on-one communications with patients, making the safety concerns from an inadvertent disclosure more substantial and the need for confidential communications more compelling. We have made the requirement for covered providers absolute and not contingent on the reason for the request because we wanted to make it relatively easy for victims of domestic violence, who face real safety concerns by disclosures of health information, to limit the potential for such disclosures.

The standard we created for health plans is different from the requirement for covered providers, in that we only require health plans to make requested accommodations for confidential communications when the individual asserts that disclosure could be dangerous to the individual. We address health plan requirements in this way because health plans are often issued to a family member (the employee), rather than to each individual member of a family, and therefore, health plans tend to communicate with the named insured rather than with individual family members. Requiring plans to accommodate a restriction for one individual could be administratively more difficult than it is for providers that regularly communicate with individuals. However, in the case of domestic violence or potential abuse, the level of harm that can result from a disclosure of protected health information tips the balance in favor of requiring such restriction to prevent inadvertent disclosure. We have adopted the policy recommended by the National Association of Insurance Commissioners in the Health Information Policy Model Act (1998) as this best reflects the balance of the appropriate level of regulation of the industry compared with the need to protect individuals from harm that may result from inadvertent disclosure of information. This policy is also consistent with recommendations made in the Family Violence Prevention Fund's publication ''Health Privacy Principles for Protecting Victims of Domestic Violence'' (October 2000). Of course, health plans may accommodate requests for confidential communications without requiring a statement that the individual would be in danger from disclosure of protected health information.

Comment: One commenter requested that we create a standard that all information from a health plan be sent to the patient and not the policyholder or subscriber.

Response: We require health plans to accommodate certain requests that information not be sent to a particular location or by particular means. A health plan must accommodate reasonable requests by individuals that protected health information about them be sent directly to them and not to a policyholder or subscriber, if the

individual states that he or she may be in danger from disclosure of such information. We did not generally require health plans to send information to the patient and not the policyholder or subscriber because we believed it would be administratively burdensome and because the named insured may have a valid need for such information to manage payment and benefits.

Sensitive Subjects

Comment: Many commenters requested that additional protections be placed on sensitive information, including information regarding HIV/AIDS, sexually transmitted diseases, mental health, substance abuse, reproductive health, and genetics. Many requested that we ensure the regulation adequately protects victims of domestic violence. They asserted that the concern for discrimination or stigma resulting from disclosure of sensitive health information could dissuade a person from seeking needed treatment. Some commenters noted that many state laws provide additional protections for various types of information. They requested that we develop federal standards to have consistent rules regarding the protection of sensitive information to achieve the goals of cost savings and patient protection. Others requested that we require patient consent or special authorization before certain types of sensitive information was disclosed, even for treatment, payment, and health care operations, and some thought we should require a separate request for each disclosure. Some commenters requested that the right to request restrictions be replaced with a requirement for an authorization for specific types of sensitive information. There were recommendations that we require covered entities to develop internal policies to address sensitive information.

Other commenters argued that sensitive information should not be segregated from the record because it may limit a future provider's access to information necessary for treatment of the individual and it could further stigmatize a patient by labeling him or her as someone with sensitive health care issues. These commenters further maintained that segregation of particular types of information could negatively affect analysis of community needs, research, and would lead to higher costs of health care delivery.

Response: We generally do not differentiate among types of protected health information, because all health information is sensitive. The level of sensitivity varies not only with the type of information, but also with the individual and the particular situation faced by the individual. This is demonstrated by the different types of information that commenters singled out as meriting special protection, and in the great variation among state laws in defining and protecting sensitive information. Most states have a law providing heightened protection for some type of health information. However, even though most states have considered the issue of sensitive information, the variation among states in the type of information that is specially protected and the requirements for permissible disclosure of such information demonstrates that there is no national consensus.

Where, as in this case, most states have acted and there is no predominant rule that emerges from the state experience with this issue, we have decided to let state law predominate. The final rule only provides a floor of protection for health information and does not preempt state laws that provide greater protection than the rule. Where states have decided to treat certain information as more sensitive than other information, we do not preempt those laws.

To address the variation in the sensitivity of protected health information without defining specially sensitive information, we incorporate opportunities for individuals and covered entities to address specific sensitivities and concerns about uses and disclosures of certain protected health information that the patient and provider believe are particularly sensitive, as follows:

- Covered entities are required to provide individuals with notice of their privacy practices and give individuals the opportunity to request restrictions of the use and disclosure of protected health information by the covered entity. (See § 164.522(a) regarding right to request restrictions.)
- Individuals have the right to request, and in some cases require, that communications from the covered entity to them be made to an alternative address or by an alternative means than the covered entity would otherwise use. (See § 164.522(b) regarding confidential communications.)
- Covered entities have the opportunity to decide not to treat a person as a personal representative when the covered entity has a reasonable belief that an individual has been subjected to domestic violence, abuse, or neglect by such person or that treating such person as a personal representative could endanger the individual. (See § 164.502(g)(5) regarding personal representatives.)
- Covered entities may deny access to protected health information when there are concerns that the access may result in varying levels of harm. (See § 164.524(a)(3) regarding denial of access.)
- Covered health care providers may, in some circumstances and consistent with any known prior preferences of the individual, exercise professional judgment in the individual's best interest to not disclose directory information. (See § 164.510(a) regarding directory information.)
- Covered entities may, in some circumstances, exercise professional judgment in the individual's best interest to limit disclosure to persons assisting in the individual's care. (See § 164.510(b) regarding persons assisting in the individual's care.)

This approach allows for state law and personal variation in this area.

The only type of protected health information that we treat with heightened protection is psychotherapy notes. We provide a different level of protection because they are unique types of protected health information that typically are not used or required for treatment, payment, or health care operations other than by the mental health professional that created the notes. (See § 164.508(a)(2) regarding psychotherapy notes.)

Section 164.524—Access of Individuals to Protected Health Information

Comment: Some commenters recommended that there be no access to disease registries.

Response: Most entities that maintain disease registries are not covered entities under this regulation; examples of such non-covered entities are public health agencies and pharmaceutical companies. If, however, a disease registry is maintained by a covered entity and is used to make decisions about individuals, this rule requires the covered entity to provide access to information about a requesting individual unless one of the rule's conditions for denial of access is met. We found no persuasive reasons why disease registries should be given special treatment compared with other information that may be used to make decisions about an individual.

Comment: Some commenters stated that covered entities should be held accountable for access to information held by business partners so that individuals would not have the burden of tracking down their protected health information from a business partner. Many commenters, including insurers

and academic medical centers, recommended that, to reduce burden and duplication, only the provider who created the protected health information should be required to provide individuals access to the information. Commenters also asked that other entities, including business associates, the Medicare program, and pharmacy benefit managers, not be required to provide access, in part because they do not know what information the covered entity already has and they may not have all the information requested. A few commenters also argued that billing companies should not have to provide access because they have a fiduciary responsibility to their physician clients to maintain the confidentiality of records.

Response: A general principle in responding to all of these points is that a covered entity is required to provide access to protected health information in accordance with the rule regardless of whether the covered entity created such information or not. Thus, we agree with the first point: in order to meet its requirements for providing access, a covered entity must not only provide access to such protected health information it holds, but must also provide access to such information in a designated record set of its business associate, pursuant to its business associate contract, unless the information is the same as information maintained directly by the covered entity. We require this because an individual may not be aware of business associate relationships. Requiring an individual to track down protected health information held by a business associate would significantly limit access. In addition, we do not permit a covered entity to limit its duty to provide access by giving protected health information to a business associate.

We disagree with the second point: if the individual directs an access request to a covered entity that has the protected health information requested, the covered entity must provide access (unless it may deny access in accordance with this rule). In order to assure that an individual can exercise his or her access rights, we do not require the individual to make a separate request to each originating provider. The originating provider may no longer be in business or may no longer have the information, or the non-originating provider may have the information in a modified or enhanced form.

We disagree with the third point: other entities must provide access only if they are covered entities or business associates of covered entities, and they must provide access only to protected health information that they maintain (or that their business associates maintain). It would not be efficient to require a covered entity to compare another entity's information with that of the entity to which the request was addressed. (See the discussion regarding covered entities for information about whether a pharmacy benefit manager is a covered entity.)

We disagree with the fourth point: a billing company will be required by its business associate contract only to provide the requested protected health information to its physician client. This action will not violate any fiduciary responsibility. The physician client would in turn be required by the rule to provide access to the individual.

Comment: Some commenters asked for clarification that the clearinghouse function of turning non-standardized data into standardized data does not create non-duplicative data and that ''duplicate'' does not mean ''identical.'' A few commenters suggested that duplicated information in a covered entity's designated record set be supplied only once per request.

Response: We consider as duplicative information the same information in different formats, media, or presentations, or which have been standardized. Business associates who have materially altered protected health information are obligated to provide individuals access to it. Summary information and reports, including those of lab results, are not the same as the underlying information on which the summaries or reports were based. A clean document is not a duplicate of the same document with notations. If the same information is kept in more than one location, the covered entity has to produce the information only once per request for access.

Comment: A few commenters suggested requiring covered entities to disclose to third parties without exception at the requests of individuals. It was argued that this would facilitate disability determinations when third parties need information to evaluate individuals' entitlement to benefits. Commenters argued that since covered entities may deny access to individuals under certain circumstances, individuals must have another method of providing third parties with their protected health information.

Response: We allow covered entities to forward protected health information about an individual to a third party, pursuant to the individual's authorization under § 164.508. We do not require covered entities to disclose information pursuant to such authorizations because the focus of the rule is privacy of protected health information. Requiring disclosures in all circumstances would be counter to this goal. In addition, a requirement of disclosing protected health information to a third party is not a necessary substitute for the right of access to individuals, because we allow denial of access to individuals under rare circumstances. However, if the third party is a personal representative of the individual in accordance with § 164.502(g) and there is no concern regarding abuse or harm to the individual or another person, we require the covered entity to provide access to that third party on the individual's behalf, subject to specific limitations. We note that a personal representative may obtain access on the individual's behalf in some cases where covered entity may deny access to the individual. For example, an inmate may be denied a copy of protected health information, but a personal representative may be able to obtain a copy on the individual's behalf. See § 164.502(g) and the corresponding preamble discussion regarding the ability of a personal representative to act on an individual's behalf.

Comment: The majority of commenters supported granting individuals the right to access protected health information for as long as the covered entity maintains the protected health information; commenters argued that to do otherwise would interfere with existing record retention laws. Some commenters advocated for limiting the right to information that is less than one or two years old. A few commenters explained that frequent changes in technology makes it more difficult to access stored data. The commenters noted that the information obtained prior to the effective date of the rule should not be required to be accessible.

Response: We agree with the majority of commenters and retain the proposal to require covered entities to provide access for as long as the entity maintains the protected health information. We do not agree that information created prior to the effective date of the rule should not be accessible. The reasons for granting individuals access to information about them do not vary with the date the information was created.

Comment: A few commenters argued that there should be no grounds for denying access, stating that individuals should always have the right to inspect and copy their protected health information.

Response: While we agree that in the vast majority of instances individuals should have access to information about them, we cannot agree that a blanket rule would be appropriate. For example, where a professional familiar with the particular circumstances believes that providing such access is likely to endanger a person's life or physical safety, or where granting such access would violate the privacy of other individuals, the benefits of allowing access may not outweigh the harm. Similarly, we allow denial of access where disclosure would reveal the source of confidential information because we do not want to interfere with a covered entity's ability to maintain implicit or explicit promises of confidence.

We create narrow exceptions to the rule of open access, and we expect covered entities to employ these exceptions rarely, if at all. Moreover, we require covered entities to provide access to any protected health information requested after excluding only the information that is subject to a denial. The categories of permissible denials are not mandatory, but are a means of preserving the flexibility and judgment of covered entities under appropriate circumstances.

Comment: Many commenters supported our proposal to allow covered entities to deny an individual access to protected health information if a professional determines either that such access is likely to endanger the life or physical safety of a person or, if the information is about another person, access is reasonably likely to cause substantial harm to such person.

Some commenters requested that the rule also permit covered entities to deny a request if access might be reasonably likely to cause psychological or mental harm, or emotional distress. Other commenters, however, were particularly concerned about access to mental health information, stating that the lack of access creates resentment and distrust in patients.

Response: We disagree with the comments suggesting that we expand the grounds for denial of access to an individual to include a likelihood of psychological or mental harm of the individual. We did not find persuasive evidence that this is a problem sufficient to outweigh the reasons for providing open access. We do allow a denial for access based on a likelihood of substantial psychological or mental harm, but only if the protected health information includes information about another person and the harm may be inflicted on such other person or if the person requesting the access is a personal representative of the individual and the harm may be inflicted on the individual or another person.

We generally agree with the commenters concerns that denying access specifically to mental health records could create distrust. To balance this concern with other commenters' concerns about the potential for psychological harm, however, we exclude psychotherapy notes from the right of access. This is the only distinction we make between mental health information and other types of protected health information in the access provisions of this rule. Unlike other types of protected health information, these notes are not widely disseminated through the health care system. We believe that the individual's privacy interests in having access to these notes, therefore, are outweighed by the potential harm caused by such access. We encourage covered entities that maintain psychotherapy notes, however, to provide individuals access to these notes when they believe it is appropriate to do so.

Comment: Some commenters believed that there is a potential for abuse of the provision allowing denial of access because of likely harm to self. They questioned whether there is any experience from the Privacy Act of 1974 to suggest that patients who requested and received their records have ever endangered themselves as a result.

Response: We are unaware of such problems from access to records that have been provided under the Privacy Act but, since these are private matters, such problems might not come to our attention. We believe it is more prudent to preserve the flexibility and judgment of health care professionals familiar with the individuals and facts surrounding a request for records than to impose the blanket rule suggested by these commenters.

Comment: Commenters asserted that the NPRM did not adequately protect vulnerable individuals who depend on others to exercise their rights under the rule. They requested that the rule permit a covered entity to deny access when the information is requested by someone other than the subject of the information and, in the opinion of a licensed health care professional, access to the information could harm the individual or another person.

Response: We agree with the commenters that such protection is warranted and add a provision in § 164.524(a)(3), which permits a covered health care provider to deny access if a personal representative of the individual is making the request for access and a licensed health care professional has determined, in the exercise of professional judgment, that providing access to such personal representative could result in substantial harm to the individual or another person. Access can be denied even if the potential harm may be inflicted by someone other than the personal representative.

This provision is designed to strike a balance between the competing interests of ensuring access to protected health information and protecting the individual or others from harm. The ''substantial harm'' standard will ensure that a covered entity cannot deny access in cases where the harm is de minimus.

The amount of discretion that a covered entity has to deny access to a personal representative is generally greater than the amount of discretion that a covered entity has to deny access to an individual. Under the final rule, a covered entity may deny access to an individual if a licensed health care professional determines that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person. In this case, concerns about psychological or emotional harm would not be sufficient to justify denial of access. We establish a relatively high threshold because we want to assure that individuals have broad access to health information about them, and due to the potential harm that comes from denial of access, we believe denials should be permitted only in limited circumstances.

The final rule grants covered entities greater discretion to deny access to a personal representative than to an individual in order to provide protection to those vulnerable people who depend on others to exercise their rights under the rule and who may be subjected to abuse or neglect. This provision applies to personal representatives of minors as well as other individuals. The same standard for denial of access on the basis of potential harm that applies to personal representatives also applies when an individual is seeking access to his or her protected health information, and the information makes reference to another person. Under these circumstances, a covered entity may deny a request for access if such access is reasonably likely to cause substantial harm to such other person. The standard for this provision and for the provision regarding access by personal representatives is the same because both circumstances involve one person obtaining information about another person, and in both cases the covered entity is balancing the right of access of one person against the right of

a second person not to be harmed by the disclosure.

Under any of these grounds for denial of access to protected health information, the covered entity is not required to deny access to a personal representative under these circumstances, but has the discretion to do so.

In addition to denial of access rights, we also address the concerns raised by abusive or potentially abusive situations in the section regarding personal representatives by giving covered entities discretion to not recognize a person as a personal representative of an individual if the covered entity has a reasonable belief that the individual has been subjected to domestic violence, abuse, or neglect by or would be in danger from a person seeking to act as the personal representative. (See § 164.502(g))

Comment: A number of commenters were concerned that this provision would lead to liability for covered entities if the release of information results in harm to individuals. Commenters requested a ''good faith'' standard in this provision to relieve covered entities of liability if individuals suffer harm as a result of seeing their protected health information or if the information is found to be erroneous. A few commenters suggested requiring providers (when applicable) to include with any disclosure to a third party a statement that, in the provider's opinion, the information should not be disclosed to the patient.

Response: We do not intend to create a new duty to withhold information nor to affect other laws on this issue. Some state laws include policies similar to this rule, and we are not aware of liability arising as a result.

Comment: Some commenters suggested that both the individual's health care professional and a second professional in the relevant field of medicine should review each request. Many commenters suggested that individuals have a right to have an independent review of any denial of access, e.g., review by a health care professional of the individual's choice.

Response: We agree with the commenters who suggest that denial on grounds of harm to self or others should be determined by a health professional, and retain this requirement in the final rule. We disagree, however, that all denials should be reviewed by a professional of the individual's choice. We are concerned that the burden such a requirement would place on covered entities would be significantly greater than any benefits to the individual. We believe that any health professional, not just one of the individual's choice, will exercise appropriate professional judgment. To address some of these concerns, however, we add a provision for the review of denials requiring the exercise of professional judgment. If a covered entity denies access based on harm to self or others, the individual has the right to have the denial reviewed by another health care professional who did not participate in the original decision to deny access.

Comment: A few commenters objected to the proposal to allow covered entities to deny a request for access to health information if the information was obtained from a confidential source that may be revealed upon the individual's access. They argued that this could be subject to abuse and the information could be inherently less reliable, making the patient's access to it even more important.

Response: While we acknowledge that information provided by confidential sources could be inaccurate, we are concerned that allowing unfettered access to such information could undermine the trust between a health care provider and patients other than the individual. We retain the proposed policy because we do not want to interfere with a covered entity's ability to obtain important information that can assist in the provision of health care or to maintain implicit or explicit promises of confidence, which may be necessary to obtain such information. We believe the concerns raised about abuse are mitigated by the fact that the provision does not apply to promises of confidentiality made to a health care provider. We note that a covered entity may provide access to such information.

Comment: Some commenters were concerned that the NPRM did not allow access to information unrelated to treatment, and thus did not permit access to research information.

Response: In the final rule, we eliminate the proposed special provision for ''research information unrelated to treatment.'' The only restriction on access to research information in this rule applies where the individual agrees in advance to denial of access when consenting to participate in research that includes treatment. In this circumstance, the individual's right of access to protected health information created in the course of the research may be suspended for as long as the research is in progress, but access rights resume after such time. In other instances, we make no distinction between research information and other information in the access provisions in this rule.

Comment: A few commenters supported the proposed provision temporarily denying access to information obtained during a clinical trial if participants agreed to the denial of access when consenting to participate in the trial. Some commenters believed there should be no access to any research information. Other commenters believed denial should occur only if the trial would be compromised. Several recommended conditioning the provision. Some recommended that access expires upon completion of the trial unless there is a health risk. A few commenters suggested that access should be allowed only if it is included in the informed consent and that the informed consent should note that some information may not be released to the individual, particularly research information that has not yet been validated. Other commenters believed that there should be access if the research is not subject to IRB or privacy board review or if the information can be disclosed to third parties.

Response: We agree with the commenters that support temporary denial of access to information from research that includes treatment if the subject has agreed in advance, and with those who suggested that the denial of access expire upon completion of the research, and retain these provisions in the final rule. We disagree with the commenters who advocate for further denial of this information. These comments did not explain why an individual's interest in access to health information used to make decisions about them is less compelling with respect to research information. Under this rule, all protected health information for research is subject either to privacy board or IRB review unless a specific authorization to use protected health information for research is obtained from the individual. Thus, this is not a criterion we can use to determine access rights.

Comment: A few commenters believed that it would be ''extremely disruptive of and dangerous'' to patients to have access to records regarding their current care and that state law provides sufficient protection of patients' rights in this regard.

Response: We do not agree. Information about current care has immediate and direct impact on individuals. Where a health care professional familiar with the circumstances believes that it is reasonably likely that access to records would endanger the life or physical safety of the individual or another

person, the regulation allows the professional to withhold access.

Comment: Several commenters requested clarification that a patient not be denied access to protected health information because of failure to pay a bill. A few commenters requested clarification that entities may not deny requests simply because producing the information would be too burdensome.

Response: We agree with these comments, and confirm that neither failure to pay a bill nor burden are lawful reasons to deny access under this rule. Covered entities may deny access only for the reasons provided in the rule.

Comment: Some commenters requested that the final rule not include detailed procedural requirements about how to respond to requests for access. Others made specific recommendations on the procedures for providing access, including requiring written requests, requiring specific requests instead of blanket requests, and limiting the frequency of requests. Commenters generally argued against requiring covered entities to acknowledge requests, except under certain circumstances, because of the potential burden on entities.

Response: We intend to provide sufficient procedural guidelines to ensure that individuals have access to their protected health information, while maintaining the flexibility for covered entities to implement policies and procedures that are appropriate to their needs and capabilities. We believe that a limit on the frequency of requests individuals may make would arbitrarily infringe on the individual's right of access and have, therefore, not included such a limitation. To limit covered entities' burden, we do not require covered entities to acknowledge receipt of the individuals' requests, other than to notify the individual once a decision on the request has been made. We also permit a covered entity to require an individual to make a request for access in writing and to discuss a request with an individual to clarify which information the individual is actually requesting. If individuals agree, covered entities may provide access to a subset of information rather than all protected health information in a designated record set. We believe these changes provide covered entities with greater flexibility without compromising individuals' access rights.

Comment: Commenters offered varying suggestions for required response time, ranging from 48 hours because of the convenience of electronic records to 60 days because of the potential burden. Others argued against a finite time period, suggesting the response time be based on mutual convenience of covered entities and individuals, reasonableness, and exigencies. Commenters also varied on suggested extension periods, from one 30-day extension to three 30-day extensions to one 90-day extension, with special provisions for off-site records.

Response: We are imposing a time limit because individuals are entitled to know when to expect a response. Timely access to protected health information is important because such information may be necessary for the individual to obtain additional health care services, insurance coverage, or disability benefits, and the covered entity may be the only source for such information. To provide additional flexibility, we eliminate the requirement that access be provided as soon as possible and we lengthen the deadline for access to off-site records. For on-site records, covered entities must act on a request within 30 days of receipt of the request. For off-site records, entities must complete action within 60 days. We also permit covered entities to extend the deadline by up to 30 days if they are unable to complete action on the request within the standard deadline. These time limits are intended to be an outside deadline rather than an expectation. We expect covered entities to be attentive to the circumstances surrounding each request and respond in an appropriate time frame.

Comment: A few commenters suggested that, upon individuals' requests, covered entities should be required to provide protected health information in a format that would be understandable to a patient, including explanations of codes or abbreviations. The commenters suggested that covered entities be permitted to provide summaries of pertinent information instead of full copies of records; for example, a summary may be more helpful for the patient's purpose than a series of indecipherable billing codes.

Response: We agree with these commenters' point that some health information is difficult to interpret. We clarify, therefore, that the covered entity may provide summary information in lieu of the underlying records. A summary may only be provided if the covered entity and the individual agree, in advance, to the summary and to any fees imposed by the covered entity for providing such summary. We similarly permit a covered entity to provide an explanation of the information. If the covered entity charges a fee for providing an explanation, it must obtain the individual's agreement to the fee in advance.

Comment: Though there were recommendations that fees be limited to the costs of copying, the majority of commenters on this topic requested that covered entities be able to charge a reasonable, cost-based fee. Commenters suggested that calculation of access costs involve factors such as labor costs for verification of requests, labor and software costs for logging of requests, labor costs for retrieval, labor costs for copying, expense costs for copying, capital cost for copying, expense costs for mailing, postal costs for mailing, billing and bad-debt expenses, and labor costs for refiling. Several commenters recommended specific fee structures.

Response: We agree that covered entities should be able to recoup their reasonable costs for copying of protected health information, and include such provision in the regulation. We are not specifying a set fee because copying costs could vary significantly depending on the size of the covered entity and the form of such copy (*e.g.,* paper, electronic, film). Rather, covered entities are permitted to charge a reasonable, cost-based fee for copying (including the costs of supplies and labor), postage, and summary or explanation (if requested and agreed to by the individual) of information supplied. The rule limits the types of costs that may be imposed for providing access to protected health information, but does not preempt applicable state laws regarding specific allowable fees for such costs. The inclusion of a copying fee is not intended to impede the ability of individuals to copy their records.

Comment: Many commenters stated that if a covered entity denies a request for access because the entity does not hold the protected health information requested, the covered entity should provide, if known, the name and address of the entity that holds the information. Some of these commenters additionally noted that the Uniform Insurance Information and Patient Protection Act, adopted by 16 states, already imposes this notification requirement on insurance entities. Some commenters also suggested requiring providers who leave practice or move offices to inform individuals of that fact and of how to obtain their records.

Response: We agree that, when covered entities deny requests for access because they do not hold the protected health information requested, they should inform individuals of the holder of the information, if known; we include this provision in the final rule. We do not require health care providers to

notify all patients when they move or leave practice, because the volume of such notifications would be unduly burdensome.

Section 164.526—Amendment of Protected Health Information

Comment: Many commenters strongly encouraged the Secretary to adopt ''appendment'' rather than ''amendment and correction'' procedures. They argued that the term ''correction'' implies a deletion of information and that the proposed rule would have allowed covered entities to remove portions of the record at their discretion. Commenters indicated that appendment rather than correction procedures will ensure the integrity of the medical record and allow subsequent health care providers access to the original information as well as the appended information. They also indicated appendment procedures will protect both individuals and covered entities since medical records are sometimes needed for litigation or other legal proceedings.

Response: We agree with commenters' concerns about the term ''correction.'' We have revised the rule and deleted ''correction'' from this provision in order to clarify that covered entities are not required by this rule to delete any information from the designated record set. We do not intend to alter medical record retention laws or current practice, except to require covered entities to append information as requested to ensure that a record is accurate and complete. If a covered entity prefers to comply with this provision by deleting the erroneous information, and applicable record retention laws allow such deletion, the entity may do so. For example, an individual may inform the entity that someone else's X-rays are in the individual's medical record. If the entity agrees that the X-ray is inaccurately filed, the entity may choose to so indicate and note where in the record the correct X-ray can be found. Alternatively, the entity may choose to remove the X-ray from the record and replace it with the correct X-ray, if applicable law allows the entity to do so. We intend the term ''amendment'' to encompass either action.

We believe this approach is consistent with well-established privacy principles, with other law, and with industry standards and ethical guidelines. The July 1977 Report of the Privacy Protection Study Commission recommended that health care providers and other organizations that maintain medical-record information have procedures for individuals to correct or amend the information.[28] The Privacy Act (5 U.S.C. 552a) requires government agencies to permit individuals to request amendment of any record the individual believes is not accurate, relevant, timely, or complete. In its report ''Best Principles for Health Privacy,'' the Health Privacy Working Group recommended, ''An individual should have the right to supplement his or her own medical record. Supplementation should not be implied to mean deletion or alteration of the medical record.'' [29] The National Association of Insurance Commissioners' Health Information Privacy Model Act establishes the right of an individual who is the subject of protected health information to amend protected health information to correct any inaccuracies. The National Conference of Commissioners on Uniform State Laws' Uniform Health Care Information Act states, ''Because accurate health-care information is not only important to the delivery of health care, but for patient applications for life, disability and health insurance, employment, and a great many other issues that might be involved in civil litigation, this Act allows a patient to request an amendment in his record.''

Some states also establish a right for individuals to amend health information about them. For example, Hawaii law (HRS section 323C–12) states, ''An individual or the individual's authorized representative may request in writing that a health care provider that generated certain health care information append additional information to the record in order to improve the accuracy or completeness of the information; provided that appending this information does not erase or obliterate any of the original information.'' Montana law (MCA section 50–16–543) states, ''For purposes of accuracy or completeness, a patient may request in writing that a health care provider correct or amend its record of the patient's health care information to which he has access.'' Connecticut, Georgia, and Maine provide individuals a right to request correction, amendment, or deletion of recorded personal information about them maintained by an insurance institution. Many other states have similar provisions.

Industry and standard-setting organizations have also developed policies for amendment of health information. The National Committee for Quality Assurance and the Joint Commission on Accreditation of Healthcare Organizations issued recommendations stating, ''The opportunity for patients to review their records will enable them to correct any errors and may provide them with a better understanding of their health status and treatment. Amending records does not erase the original information. It inserts the correct information with a notation about the date the correct information was available and any explanation about the reason for the error.'' [30] Standards of the American Society for Testing and Materials state, ''An individual has a right to amend by adding information to his or her record or database to correct inaccurate information in his or her patient record and in secondary records and databases which contain patient identifiable health information.'' [31] We build on this well-established principle in this final rule.

Comment: Some commenters supported the proposal to allow individuals to request amendment for as long as the covered provider or plan maintains the information. A few argued that the provision should be time-limited, *e.g.,* that covered entities should not have to amend protected health information that is more than two years old. Other comments suggested that the provision should only be applied to protected health information created after the compliance date of the regulation.

Response: The purpose of this provision is to create a mechanism whereby individuals can ensure that information about them is as accurate as possible as it travels through the health care system and is used to make decisions, including treatment decisions, about them. To achieve this result, individuals must have the ability to request amendment for as long as the information used to make decisions about them exists. We therefore retain the proposed approach. For these reasons, we also require covered entities to address requests for amendment of all protected health information within designated record sets, including information created or obtained prior to

[28] Privacy Protection Study Commission, ''Personal Privacy in an Information Society,'' July 1977, p. 300–303.

[29] Health Privacy Working Group, ''Best Principles for Health Privacy,'' Health Privacy Project, Institute for Health Care Research and Policy, Georgetown University, July 1999.

[30] National Committee on Quality Assurance and the Joint Commission on Accreditation of Healthcare Organizations, ''Protecting Personal Health Information: A Framework for Meeting the Challenges in a Managed Care Environment,''1998, p. 25.

[31] ASTM, ''Standard Guide for Confidentiality, Privacy, Access and Data Security, Principles for Health Information Including Computer-Based Patient Records,'' E 1869–97, § 11.1.1.

the compliance date, for as long as the entity maintains the information.

Comment: A few commenters were concerned that the proposal implied that the individual is in control of and may personally change the medical record. These commenters opposed such an approach.

Response: We do not give individuals the right to alter their medical records. Individuals may request amendment, but they have no authority to determine the final outcome of the request and may not make actual changes to the medical record. The covered entity must review the individual's request and make appropriate decisions. We have clarified this intent in § 164.526(a)(1) by stating that individuals have a right to have a covered entity amend protected health information and in § 164.526(b)(2) by stating that covered entities must act on an individual's request for amendment.

Comment: Some comments argued that there is no free-text field in some current transaction formats that would accommodate the extra text required to comply with the amendment provisions (*e.g.,* sending statements of disagreement along with all future disclosures of the information at issue). Commenters argued that this provision will burden the efficient transmission of information, contrary to HIPAA requirements.

Response: We believe that most amendments can be incorporated into the standard transactions as corrections of erroneous data. We agree that some of the standard transactions cannot currently accommodate additional material such as statements of disagreement and rebuttals to such statements. To accommodate these rare situations, we modify the requirements in § 164.526(d)(iii). The provision now states that if a standard transaction does not permit the inclusion of the additional material required by this section, the covered entity may separately transmit the additional material to the recipient of the standard transaction. Commenters interested in modifying the standard transactions to allow the incorporation of additional materials may also bring the issue up for resolution through the process established by the Transactions Rule and described in its preamble.

Comment: The NPRM proposed to allow amendment of protected health information in designated record sets. Some commenters supported the concept of a designated record set and stated that it appropriately limits the type of information available for amendment to information directly related to treatment. Other commenters were concerned about the burden this provision will create due to the volume of information that will be available for amendment. They were primarily concerned with the potential for frivolous, minor, or technical requests. They argued that for purposes of amendment, this definition should be limited to information used to make medical or treatment decisions about the individual. A few commenters requested clarification that individuals do not have a right to seek amendment unless there is verifiable information to support their claim or they can otherwise convince the entity that the information is inaccurate or incomplete.

Response: We believe that the same information available for inspection should also be subject to requests for amendment, because the purpose of these provisions is the same: To give consumers access to and the chance to correct errors in information that may be used to make decisions that affect their interests. We thus retain use of the ''designated record set'' in this provision. However, we share commenters'' concerns about the potential for minor or technical requests. To address this concern, we have clarified that covered entities may deny a request for amendment if the request is not in writing and does not articulate a reason to support the request, as long as the covered entity informs the individual of these requirements in advance.

Comment: Many commenters noted the potentially negative impact of the proposal to allow covered entities to deny a request for amendment if the covered entity did not create the information at issue. Some commenters pointed out that the originator of the information may no longer exist or the individual may not know who created the information in question. Other commenters supported the proposal that only the originator of the information is responsible for amendments to it. They argued that any extension of this provision requiring covered entities to amend information they have not created is administratively and financially burdensome.

Response: In light of the comments, we modify the rule to require the holder of the information to consider a request for amendment if the individual requesting amendment provides a reasonable basis to believe that the originator of the information is no longer available to act on a request. For example, if a request indicates that the information at issue was created by a hospital that has closed, and the request is not denied on other grounds, then the entity must amend the information. This provision is necessary to preserve an individual's right to amend protected health information about them in certain circumstances.

Comment: Some commenters stated that the written contract between a covered entity and its business associate should stipulate that the business associate is required to amend protected health information in accordance with the amendment provisions. Otherwise, these commenters argued, there would be a gap in the individual's right to have erroneous information corrected, because the covered entity could deny a request for amendment of information created by a business associate.

Response: We agree that information created by the covered entity or by the covered entity's business associates should be subject to amendment. This requirement is consistent with the requirement to make information created by a business associate available for inspection and copying. We have revised the rule to require covered entities to specify in the business associate contract that the business associate will make protected health information available for amendment and will incorporate amendments accordingly. (See § 164.504(e).)

Comment: One commenter argued that covered entities should be required to presume information must be corrected where an individual informs the entity that an adjudicative process has made a finding of medical identity theft.

Response: Identity theft is one of many reasons why protected health information may be inaccurate, and is one of many subjects that may result in an adjudicative process relevant to the accuracy of protective health information. We believe that this provision accommodates this situation without a special provision for identity theft.

Comment: Some commenters asserted that the proposed rule's requirement that action must be taken on individuals' requests within 60 days of the receipt of the request was unreasonable and burdensome. A few commenters proposed up to three 30-day extensions for ''extraordinary'' (as defined by the entity) requests.

Response: We agree that 60 days will not always be a sufficient amount of time to adequately respond to these requests. Therefore, we have revised this provision to allow covered entities the option of a 30-day extension to deal with requests that require additional response time. However, we expect that 60 days will be adequate for most cases.

Comment: One commenter questioned whether a covered entity could

appropriately respond to a request by amending the record, without indicating whether it believes the information at issue is accurate and complete.

Response: An amendment need not include a statement by the covered entity as to whether the information is or is not accurate and complete. A covered entity may choose to amend a record even if it believes the information at issue is accurate and complete. If a request for amendment is accepted, the covered entity must notify the individual that the record has been amended. This notification need not include any explanation as to why the request was accepted. A notification of a denied request, however, must contain the basis for the denial.

Comment: A few commenters suggested that when an amendment is made, the date should be noted. Some also suggested that the physician should sign the notation.

Response: We believe such a requirement would create a burden that is not necessary to protect individuals' interests, and so have not accepted this suggestion. We believe that the requirements of § 164.526(c) regarding actions a covered entity must take when accepting a request will provide an adequate record of the amendment. A covered entity may date and sign an amendment at its discretion.

Comment: The NPRM proposed that covered entities, upon accepting a request for amendment, make reasonable efforts to notify those persons the individual identifies, and other persons whom the covered entity knows have received the erroneous or incomplete information and who may have relied, or could foreseeably rely, on such information to the detriment of the individual. Many commenters argued that this notification requirement was too burdensome and should be narrowed. They expressed concern that covered entities would have to notify anyone who might have received the information, even persons identified by the individual with whom the covered entity had no contact. Other commenters also contended that this provision would require covered entities to determine the reliance another entity might place on the information and suggested that particular part of the notification requirements be removed. Another commenter suggested that the notification provision be eliminated entirely, believing that it was unnecessary.

Response: Although there is some associated administrative burden with this provision, we believe it is a necessary requirement to effectively communicate amendments of erroneous or incomplete information to other parties. The negative effects of erroneous or incomplete medical information can be devastating. This requirement allows individuals to exercise some control in determining recipients they consider important to be notified, and requires the covered entity to communicate amendments to other persons that the covered entity knows have the erroneous or incomplete information and may take some action in reliance on the erroneous or incomplete information to the detriment of the individual. We have added language to clarify that the covered entity must obtain the individual's agreement to have the amendment shared with the persons the individual and covered entity identifies. We believe these notification requirements appropriately balance covered entities' burden and individuals' interest in protecting the accuracy of medical information used to make decisions about them. We therefore retain the notification provisions substantially as proposed.

Comment: Some commenters argued against the proposed provision requiring a covered entity that receives a notice of amendment to notify its business associates, ''as appropriate,'' of necessary amendments. Some argued that covered entities should only be required to inform business associates of these changes if the amendment could affect the individual's further treatment, citing the administrative and financial burden of notifying all business associates of changes that may not have a detrimental effect on the patient. Other commenters suggested that covered entities should only be required to inform business associates whom they reasonably know to be in possession of the information.

Response: We agree with commenters that clarification is warranted. Our intent is that covered entities must meet the requirements of this rule with respect to protected health information they maintain, including protected health information maintained on their behalf by their business associates. We clarify this intent by revising the definition of designated record set (see § 164.501) to include records maintained ''by or for'' a covered entity. Section 164.526(e) requires a covered entity that is informed of an amendment made by another covered entity to incorporate that amendment into designated record sets, whether the designated record set is maintained by the covered entity or for the covered entity by a business associate. If a business associate maintains the record at issue on the covered entity's behalf, the covered entity must fulfill its requirement by informing the business associate of the amendment to the record. The contract with the business associate must require the business associate to incorporate any such amendments. (See § 164.504(e).)

Comment: Some commenters supported the proposal to require covered entities to provide notification of the covered entity's statement of denial and the individual's statement of disagreement in any subsequent disclosures of the information to which the dispute relates. They argued that we should extend this provision to prior recipients of disputed information who have relied on it. These commenters noted an inconsistency in the proposed approach, since notification of accepted amendments is provided to certain previous recipients of erroneous health information and to recipients of future disclosures. They contended there is not a good justification for the different treatment and believed that the notification standard should be the same, regardless of whether the covered entity accepts the request for amendment.

These commenters also recommended that the individual be notified of the covered entity's intention to rebut a statement of disagreement. They suggested requiring covered entities to send a copy of the statement of rebuttal to the individual.

Response: Where a request for amendment is accepted, the covered entity knows that protected health information about the individual is inaccurate or incomplete or the amendment is otherwise warranted; in these circumstances, it is reasonable to ask the covered entity to notify certain previous recipients of the information that reliance on such information could be harmful. Where, however, the request for amendment is denied, the covered entity believes that the relevant information is accurate and complete or the amendment is otherwise unacceptable. In this circumstance, the burden of prior notification outweighs the potential benefits. We therefore do not require notification of prior recipients.

We agree, however, that individuals should know how a covered entity has responded to their requests, and therefore add a requirement that covered entities also provide a copy of any rebuttal statements to the individual.

Section 164.528—Accounting of Disclosures of Protected Health Information

Comment: Many commenters expressed support for the concept of the right to receive an accounting of disclosures. Others opposed even the concept. One commenter said that it is likely that some individuals will request an accounting of disclosures from each of his or her health care providers and payors merely to challenge the disclosures that the covered entity made.

Some commenters also questioned the value to the individual of providing the right to an accounting. One commenter stated that such a provision would be meaningless because those who deliberately perpetrate an abuse are unlikely to note their breach in a log.

Response: The final rule retains the right of an individual to receive an accounting of disclosures of protected health information. The provision serves multiple purposes. It provides a means of informing the individual as to which information has been sent to which recipients. This information, in turn, enables individuals to exercise certain other rights under the rule, such as the rights to inspection and amendment, with greater precision and ease. The accounting also allows individuals to monitor how covered entities are complying with the rule. Though covered entities who deliberately make disclosures in violation of the rule may be unlikely to note such a breach in the accounting, other covered entities may document inappropriate disclosures that they make out of ignorance and not malfeasance. The accounting will enable the individual to address such concerns with the covered entity.

We believe this approach is consistent with well-established privacy principles, with other law, and with industry standards and ethical guidelines. The July 1977 Report of the Privacy Protection Study Commission recommended that a health care provider should not disclose individually-identifiable information for certain purposes without the individual's authorization unless ''an accounting of such disclosures is kept and the individual who is the subject of the information being disclosed can find out that the disclosure has been made and to whom.'' [32] With certain exceptions, the Privacy Act (5 U.S.C. 552a) requires government agencies to ''keep an accurate accounting of * * * the date, nature, and purpose of each disclosure of a record to any person or to another agency * * * and * * * the name and address of the person or agency to whom the disclosure is made.'' The National Association of Insurance Commissioners' Health Information Privacy Model Act requires carriers to provide to individuals on request ''information regarding disclosure of that individual's protected health information that is sufficient to exercise the right to amend the information.'' We build on these standards in this final rule.

Comment: Many commenters disagreed with the NPRM's exception for treatment, payment, and health care operations. Some commenters wanted treatment, payment, and health care operations disclosures to be included in an accounting because they believed that improper disclosures of protected health information were likely to be committed by parties within the entity who have access to protected health information for treatment, payment, and health care operations related purposes. They suggested that requiring covered entities to record treatment, payment, and health care operations disclosures would either prevent improper disclosures or enable transgressions to be tracked.

One commenter reasoned that disclosures for treatment, payment, and health care operations purposes should be tracked since these disclosures would be made without the individual's consent. Others argued that if an individual's authorization is not required for a disclosure, then the disclosure should not have to be tracked for a future accounting to the individual.

One commenter requested that the provision be restated so that no accounting is required for disclosures ''compatible with or directly related to'' treatment, payment or health care operations. This comment indicated that the change would make § 164.515(a)(1) of the NPRM consistent with § 164.508(a)(2)(i)(A) of the NPRM.

Response: We do not accept the comments suggesting removing the exception for disclosures for treatment, payment, and health care operations. While including all disclosures within the accounting would provide more information to individuals about to whom their information has been disclosed, we believe that documenting all disclosures made for treatment, payment, and health care operations purposes would be unduly burdensome on entities and would result in accountings so voluminous as to be of questionable value. Individuals who seek treatment and payment expect that their information will be used and disclosed for these purposes. In many cases, under this final rule, the individual will have consented to these uses and disclosures. Thus, the additional information that would be gained from including these disclosures would not outweigh the added burdens on covered entities. We believe that retaining the exclusion of disclosures to carry out treatment, payment, and health care operations makes for a manageable accounting both from the point of view of entities and of individuals. We have conformed the language in this section with language in other sections of the rule regarding uses and disclosures to carry out treatment, payment, and health care operations. See § 164.508 and the corresponding preamble discussion regarding our decision to use this language.

Comments: A few commenters called for a record of all disclosures, including a right of access to a full audit trail where one exists. Some commenters stated while audit trails for paper records are too expensive to require, the privacy rule should not discourage audit trails, at least for computer-based records. They speculated that an important reason for maintaining a full audit trail is that most abuses are the result of activity by insiders. On the other hand, other commenters pointed out that an enormous volume of records would be created if the rule requires recording all accesses in the manner of a full audit trail.

One commenter supported the NPRM's reference to the proposed HIPAA Security Rule, agreeing that access control and disclosure requirements under this rule should be coordinated with the final HIPAA Security Rule. The commenter recommended that HHS add a reference to the final HIPAA Security Rule in this section and keep specific audit log and reporting requirements generic in the privacy rule.

Response: Audit trails and the accounting of disclosures serve different functions. In the security field, an audit trail is typically a record of each time a sensitive record is altered, how it was altered and by whom, but does not usually record each time a record is used or viewed. The accounting required by this rule provides individuals with information about to whom a disclosure is made. An accounting, as described in this rule, would not capture uses. To the extent that an audit trail would capture uses, consumers reviewing an audit trail may not be able to distinguish between

[32] Privacy Protection Study Commission, ''Personal Privacy in an Information Society,'' July 1977, pp. 306–307.

accesses of the protected health information for use and accesses for disclosure. Further, it is not clear the degree to which the field is technologically poised to provide audit trails. Some entities could provide audit trails to individuals upon their request, but we are concerned that many could not.

We agree that it is important to coordinate this provision of the privacy rule with the Security Rule when it is issued as a final rule.

Comments: We received many comments from researchers expressing concerns about the potential impact of requiring an accounting of disclosures related to research. The majority feared that the accounting provision would prove so burdensome that many entities would decline to participate in research. Many commenters believed that disclosure of protected health information for research presents little risk to individual privacy and feared that the accounting requirement could shut down research.

Some commenters pointed out that often only a few data elements or a single element is extracted from the patient record and disclosed to a researcher, and that having to account for so singular a disclosure from what could potentially be an enormous number of records imposes a significant burden. Some said that the impact would be particularly harmful to longitudinal studies, where the disclosures of protected health information occur over an extended period of time. A number of commenters suggested that we not require accounting of disclosures for research, registries, and surveillance systems or other databases unless the disclosure results in the actual physical release of the patient's entire medical record, rather than the disclosure of discrete elements of information contained within the record.

We also were asked by commenters to provide an exclusion for research subject to IRB oversight or research that has been granted a waiver of authorization pursuant to proposed § 164.510, to exempt ''in-house'' research from the accounting provision, and to allow covered entities to describe the type of disclosures they have made to research projects, without specifically listing each disclosure. Commenters suggested that covered entities could include in an accounting a listing of the various research projects in which they participated during the time period at issue, without regard to whether a particular individual's protected health information was disclosed to the project.

Response: We disagree with suggestions from commenters that an accounting of disclosures is not necessary for research. While it is possible that informing individuals about the disclosures made of their health information may on occasion discourage worthwhile activities, we believe that individuals have a right to know who is using their health information and for what purposes. This information gives individuals more control over their health information and a better base of knowledge from which to make informed decisions.

For the same reasons, we also do not believe that IRB or privacy board review substitutes for providing individuals the right to know how their information has been disclosed. We permit IRBs or privacy boards to determine that a research project would not be feasible if authorization were required because we understand that it could be virtually impossible to get authorization for archival research involving large numbers of individuals or where the location of the individuals is not easy to ascertain. While providing an accounting of disclosures for research may entail some burden, it is feasible, and we do not believe that IRBs or privacy boards would have a basis for waiving such a requirement. We also note that the majority of comments that we received from individuals supported including more information in the accounting, not less.

We understand that requiring covered entities to include disclosures for research in the accounting of disclosures entails some burden, but we believe that the benefits described above outweigh the burden.

We do not agree with commenters that we should exempt disclosures where only a few data elements are released or in the case of data released without individuals' names. We recognize that information other than names can identify an individual. We also recognize that even a few data elements could be clues to an individual's identity. The actual volume of information released is not an appropriate indicator of whether an individual could have a concern about privacy.

We disagree with comments that suggested that it would be sufficient to provide individuals with a general list of research projects to which information has been disclosed by the covered entity. We believe that individuals are entitled to a level of specificity about disclosures of protected health information about them and should know to which research projects their protected health information has been disclosed, rather than to which projects protected health information may have been disclosed. However, we have added a provision allowing for a summary accounting of recurrent disclosures. For multiple disclosures to the same recipient pursuant to a single authorization or for a single purpose permitted under the rule without authorization, the covered entity may provide a summary accounting addressing the series of disclosures rather than a detailed accounting of each disclosure in the series. This change is designed to ease the burden on covered entities involved in longitudinal projects.

With regard to the suggestion that we exempt ''in-house'' research from the accounting provision, we note that only disclosures of protected health information must appear in an accounting.

Comments: Several commenters noted that disclosures for public health activities may be of interest to individuals, but add to the burden imposed on entities. Furthermore, some expressed fear that priority public health activities would be compromised by the accounting provision. One commenter from a health department said that covered entities should not be required to provide an accounting to certain index cases, where such disclosures create other hazards, such as potential harm to the reporting provider. This commenter also speculated that knowing protected health information had been disclosed for these public health purposes might cause people to avoid treatment in order to avoid being reported to the public health department.

A provider association expressed concern about the effect that the accounting provision might have on a non-governmental, centralized disease registry that it operates. The provider organization feared that individuals might request that their protected health information be eliminated in the databank, which would make the data less useful.

Response: As in the discussion of research above, we reject the contention that we should withhold information from individuals about where their information has been disclosed because informing them could occasionally discourage some worthwhile activities. We also believe that, on balance, individuals' interest in having broad access to this information outweighs concerns about the rare instances in which providing this information might raise concerns about harm to the person who made the disclosure. As we stated above, we believe that individuals have

a right to know who is using their health information and for what purposes. This information gives individuals more control over their health information and a better base of knowledge from which to make informed decisions.

Comment: We received many comments about the proposed time-limited exclusion for law enforcement and health oversight. Several commenters noted that it is nearly impossible to accurately project the length of an investigation, especially during its early stages. Some recommended we permit a deadline based on the end of an event, such as conclusion of an investigation. One commenter recommended amending the standard such that covered entities would never be required to give an accounting of disclosures to health oversight or law enforcement agencies. The commenter noted that there are public policy reasons for limiting the extent to which a criminal investigation is made known publicly, including the possibility that suspects may destroy or falsify evidence, hide assets, or flee. The commenter also pointed out that disclosure of an investigation may unfairly stigmatize a person or entity who is eventually found to be innocent of any wrongdoing.

On the other hand, many commenters disagreed with the exemption for recording disclosures related to oversight activities and law enforcement. Many of these commenters stated that the exclusion would permit broad exceptions for government purposes while holding disclosures for private purposes to a more burdensome standard.

Some commenters felt that the NPRM made it too easy for law enforcement to obtain an exception. They suggested that law enforcement should not be excepted from the accounting provision unless there is a court order. One commenter recommended that a written request for exclusion be dated, signed by a supervisory official, and contain a certification that the official is personally familiar with the purpose of the request and the justification for exclusion from accounting.

Response: We do not agree with comments suggesting that we permanently exclude disclosures for oversight or law enforcement from the accounting. We believe generally that individuals have a right to know who is obtaining their health information and for what purposes.

At the same time, we agree with commenters that were concerned that an accounting could tip off subjects of investigations. We have retained a time-limed exclusion period similar to that proposed in the NPRM. To protect the integrity of investigations, in the final rule we require covered entities to exclude disclosures to a health oversight agency or law enforcement official for the time specified by that agency or official, if the agency or official states that including the disclosure in an accounting to the individual would be reasonably likely to impede the agency or official's activities. We require the statement from the agency or official to provide a specific time frame for the exclusion. For example, pursuant to a law enforcement official's statement, a covered entity could exclude a law enforcement disclosure from the accounting for a period of three months from the date of the official's statement or until a date specified in the statement.

In the final rule, we permit the covered entity to exclude the disclosure from an accounting to an individual if the agency or official makes the statement orally and the covered entity documents the statement and the identify of the agency or official that made the statement. We recognize that in urgent situations, agencies and officials may not be able to provide statements in writing. If the agency or official's statement is made orally, however, the disclosure can be excluded from an accounting to the individual for no longer than 30 days from the oral statement. For exclusions longer than 30 days, a covered entity must receive a written statement.

We believe these requirements appropriately balance individuals' rights to be informed of the disclosures of protected health information while recognizing the public's interest in maintaining the integrity of health oversight and law enforcement activities.

Comment: One commenter stated that under Minnesota law, providers who are mandated reporters of abuse are limited as to whom they may reveal the report of abuse (generally law enforcement authorities and other providers only). This is because certain abusers, such as parents, by law may have access to a victim's (child's) records. The commenter requested clarification as to whether these disclosures are exempt from the accounting requirement or whether preemption would apply.

Response: While we do not except mandatory disclosures of abuse from the accounting for disclosure requirement, we believe the commenter's concerns are addressed in several ways. First, nothing in this regulation invalidates or limits the authority or procedures established under state law providing for the reporting of child abuse. Thus, with respect to child abuse the Minnesota law's procedures are not preempted even though they are less stringent with respect to privacy. Second, with respect to abuse of persons other than children, we allow covered entities to refuse to treat a person as an individual's personal representative if the covered entity believes that the individual has been subjected to domestic violence, abuse, or neglect from the person. Thus, the abuser would not have access to the accounting. We also note that a covered entity must exclude a disclosure, including disclosures to report abuse, from the accounting for specified period of time if the law enforcement official to whom the report is made requests such exclusion.

Comment: A few comments noted the lack of exception for disclosures made to intelligence agencies.

Response: We agree with the comments and have added an exemption for disclosures made for national security or intelligence purposes under § 164.512(k)(2). Individuals do not have a right to an accounting of disclosures for these purposes.

Comment: Commenters noted that the burden associated with this provision would, in part, be determined by other provisions of the rule, including the definitions of ''individually identifiable,'' ''treatment,'' and ''health care operations.'' They expressed concern that the covered entity would have to be able to organize on a patient by patient basis thousands of disclosures of information, which they described as ''routine.'' These commenters point to disclosures for patient directory information, routine banking and payment processes, uses and disclosures in emergency circumstances, disclosures to next of kin, and release of admissions statistics to a health oversight agency.

Response: We disagree with the commenters that ambiguity in other areas of the rule increase the burden associated with maintaining an accounting. The definitions of treatment, payment, and health operations are necessarily broad and there is no accounting required for disclosures for these purposes. These terms cover the vast majority of routine disclosures for health care purposes. (See § 164.501 and the associated preamble for a discussion of changes made to these definitions.)

The disclosures permitted under § 164.512 are for national priority purposes, and determining whether a disclosure fits within the section is necessary before the disclosure can be

made. There is no additional burden, once such a determination is made, in determining whether it must be included in the accounting.

We agree with the commenters that there are areas where we can reduce burden by removing additional disclosures from the accounting requirement, without compromising individuals' rights to know how their information is being disclosed. In the final rule, covered entities are not required to include the following disclosures in the accounting: disclosures to the individual, disclosures for facility directories under § 164.510(a), or disclosures to persons assisting in the individual's care or for other notification purposes under § 164.510(b). For each of these types of disclosures, the individual is likely to already know about the disclosure or to have agreed to the disclosure, making the inclusion of such disclosures in the accounting less important to the individual and unnecessarily burdensome to the covered entity.

Comment: Many commenters objected to requiring business partners to provide an accounting to covered entities upon their request. They cited the encumbrance associated with re-contracting with the various business partners, as well as the burden associated with establishing this type of record keeping.

Response: Individuals have a right to know to whom and for what purpose their protected health information has been disclosed by a covered entity. The fact that a covered entity uses a business associate to carry out a function does not diminish an individual's right to know.

Comments: One commenter requested clarification as to how far a covered entity's responsibility would extend, asking whether an entity had to track only their direct disclosures or subsequent re-disclosures.

Response: Covered entities are required to account for their disclosures, as well as the disclosures of their business associates, of protected health information. Because business associates act on behalf of covered entities, it is essential that their disclosures be included in any accounting that an individual requests from a covered entity. Covered entities are not responsible, however, for the actions of persons who are not their business associates. Once a covered entity has accounted for a disclosure to any person other than a business associate, it is not responsible for accounting for any further uses or disclosures of the information by that other person.

Comments: Some commenters said that the accounting provision described in the NPRM was ambiguous and created uncertainty as to whether it addresses disclosures only, as the title would indicate, or whether it includes accounting of uses. They urged that the standard address disclosures only, and not uses, which would make implementation far more practicable and less burdensome.

Response: The final rule requires disclosures, not uses, to be included in an accounting. See § 164.501 for definitions of ''use'' and ''disclosure.''

Comments: We received many comments from providers and other representatives of various segments of the health care industry, expressing the view that a centralized system of recording disclosures was not possible given the complexity of the health care system, in which disclosures are made by numerous departments within entities. For example, commenters stated that a hospital medical records department generally makes notations regarding information it releases, but that these notations do not include disclosures that the emergency department may make. Several commenters proposed that the rule provide for patients to receive only an accounting of disclosures made by medical records departments or some other central location, which would relieve the burden of centralizing accounting for those entities who depend on paper records and tracking systems.

Response: We disagree with commenters' arguments that covered entities should not be held accountable for the actions of their subdivisions or workforce members. Covered entities are responsible for accounting for the disclosures of protected health information made by the covered entity, in accordance with this rule. The particular person or department within the entity that made the disclosure is immaterial to the covered entity's obligation. In the final rule, we require covered entities to document each disclosure that is required to be included in an accounting. We do not, however, require this documentation to be maintained in a central registry. A covered hospital, for example, could maintain separate documentation of disclosures that are made from the medical records department and the emergency department. At the time an individual requests an accounting, this documentation could be integrated to provide a single accounting of disclosures made by the covered hospital. Alternatively, the covered hospital could centralize its processes for making and documenting disclosures. We believe this provision provides covered entities with sufficient flexibility to meet their business needs without compromising individuals' rights to know how information about them is disclosed.

Comments: Commenters stated that the accounting requirements placed undue burden on covered entities that use paper, rather than electronic, records.

Response: We do not agree that the current reliance on paper records makes the accounting provision unduly burdensome. Covered entities must use the paper records in order to make a disclosure, and have the opportunity when they do so to make a notation in the record or in a separate log. We require an accounting only for disclosures for purposes other than treatment, payment, and health care operations. Such disclosures are not so numerous that they cannot be accounted for, even if paper records are involved.

Comments: The exception to the accounting provision for disclosures of protected health information for treatment, payment, and health care operations purposes was viewed favorably by many respondents. However, at least one commenter stated that since covered entities must differentiate between disclosures that require documentation and those that do not, they will have to document each instance when a patient's medical record is disclosed to determine the reason for the disclosure. This commenter also argued that the administrative burden of requiring customer services representatives to ask in which category the information falls and then to keep a record that they asked the question and record the answer would be overwhelming for plans. The commenter concluded that the burden of documentation on a covered entity would not be relieved by the stipulation that documentation is not required for treatment, payment, and health care operations.

Response: We disagree. Covered entities are not required to document every disclosure in order to differentiate those for treatment, payment, and health care operations from those for purposes for which an accounting is required. We require that, when a disclosure is made for which an accounting is required, the covered entity be able to produce an accounting of those disclosures upon request. We do not require a covered entity to be able to account for every disclosure. In addition, we believe that we have addressed many of the commenters' concerns by clarifying in the final rule that disclosures to the

individual, regardless of the purpose for the disclosure, are not subject to the accounting requirement.

Comments: An insurer explained that in the context of underwriting, it may have frequent and multiple disclosures of protected health information to an agent, third party medical provider, or other entity or individual. It requested we reduce the burden of accounting for such disclosures.

Response: We add a provision allowing for a summary accounting of recurrent disclosures. For multiple disclosures to the same recipient pursuant to a single authorization or for a single purpose permitted under the rule without authorization, the covered entity may provide a summary accounting addressing the series of disclosures rather than a detailed accounting of each disclosure in the series.

Comment: Several commenters said that it was unreasonable to expect covered entities to track disclosures that are requested by the individual. They believed that consumers should be responsible for keeping track of their own requests.

Other commenters asked that we specify that entities need not retain and provide copies of the individual's authorization to disclose protected health information. Some commenters were particularly concerned that if they maintain all patient information on a computer system, it would be impossible to link the paper authorization with the patient's electronic records.

Another commenter suggested we allow entities to submit copies of authorizations after the 30-day deadline for responding to the individual, as long as the accounting itself is furnished within the 30-day window.

Response: In the final rule we do not require disclosures to the individual to be included in the accounting. Other disclosures requested by the individual must be included in the accounting, unless they are otherwise excepted from the requirement. We do not agree that individuals should be required to track these disclosures themselves. In many cases, an authorization may authorize a disclosure by more than one entity, or by a class of entities, such as all physicians who have provided medical treatment to the individual. Absent the accounting, the individual cannot know whether a particular covered entity has acted on the authorization.

We agree, however, that it is unnecessarily burdensome to require covered entities to provide the individual with a copy of the authorization. We remove the requirement. Instead, we require the accounting to contain a brief statement describing the purpose for which the protected health information was disclosed. The statement must be sufficient to reasonably inform the individual of the basis for the disclosure. Alternatively, the covered entity may provide a copy of the authorization or a copy of the written request for disclosure, if any, under §§ 164.502(a)(2)(ii) or 164.512.

Comments: We received many comments regarding the amount of information required in the accounting. A few commenters requested that we include additional elements in the accounting, such as the method of transmittal and identity of the employee who accessed the information.

Other commenters, however, felt that the proposed requirements went beyond what is necessary to inform the individual of disclosures. Another commenter stated that if the individual's right to obtain an accounting extends to disclosures that do not require a signed authorization, then the accounting should be limited to a disclosure of the manner and purpose of disclosures, as opposed to an individual accounting of each entity to whom the protected health information was disclosed. An insurer stated that this section of the proposed rule should be revised to provide more general, rather than detailed, guidelines for accounting of disclosures. The commenter believed that its type of business should be allowed to provide general information regarding the disclosure of protected health information to outside entities, particularly with regard to entities with which the insurer maintains an ongoing, standard relationship (such as a reinsurer).

Response: In general, we have retained the proposed approach, which we believe strikes an appropriate balance between the individual's right to know to whom and for what purposes their protected health information has been disclosed and the burden placed on covered entities. In the final rule, we clarify that the accounting must include the address of the recipient only if the address is known to the covered entity. As noted above, we also add a provision allowing for a summary accounting of recurrent disclosures. We note that some of the activities of concern to commenters may fall under the definition of health care operations (see § 164.501 and the associated preamble).

Comment: A commenter asked that we limit the accounting to information pertaining to the medical record itself, as opposed to protected health information more generally. Similarly, commenters suggested that the accounting be limited to release of the medical record only.

Response: We disagree. Protected health information exists in many forms and resides in many sources. An individual's right to know to whom and for what purposes his or her protected health information has been disclosed would be severely limited if it pertained only to disclosure of the medical record, or information taken only from the record.

Comment: A commenter asked that we make clear that only disclosures external to the organization are within the accounting requirement.

Response: We agree. The requirement only applies to disclosures of protected health information, as defined in § 164.501.

Comment: Some commenters requested that we establish a limit on the number of times an individual could request an accounting. One comment suggested we permit individuals to request one accounting per year; another suggested two accountings per year, except in ''emergency situations.'' Others recommended that we enable entities to recoup some of the costs associated with implementation by allowing the entity to charge for an accounting.

Response: We agree that covered entities should be able to defray costs of excessive requests. The final rule provides individuals with the right to receive one accounting without charge in a twelve-month period. For additional requests by an individual within a twelve-month period, the covered entity may charge a reasonable, cost-based fee. If it imposes such a fee, the covered entity must inform the individual of the fee in advance and provide the individual with an opportunity to withdraw or modify the request to avoid or reduce the fee.

Comment: In the NPRM, we solicited comments on the appropriate duration of the individual's right to an accounting. Some commenters supported the NPRM's requirement that the right exist for as long as the covered entities maintains the protected health information. One commenter, however, noted that most audit control systems do not retain data on activity for indefinite periods of time.

Other commenters noted that laws governing the length of retention of clinical records vary by state and by provider type and suggested that entities be allowed to adhere to state laws or policies established by professional organizations or accrediting bodies. Some commenters suggested that the

language be clarified to state that whatever minimum requirements are in place for the record should also guide covered entities in retaining their capacity to account for disclosures over that same time, but no longer.

Several commenters asked us to consider specific time limits. It was pointed out that proposed § 164.520(f)(6) of the NPRM set a six-year time limit for retaining certain information including authorization forms and contracts with business partners. Included in this list was the accounting of disclosures, but this requirement was inconsistent with the more open-ended language in § 164.515. Commenters suggested that deferring to this six-year limit would make this provision consistent with other record retention provisions of the standard and might relieve some of the burden associated with implementation. Other specific time frames suggested were two years, three years, five years, and seven years.

Another option suggested by commenters was to keep the accounting record for as long as entities have the information maintained and ''active'' on their systems. Information permanently taken off the covered entity's system and sent to ''dead storage'' would not be covered. One commenter further recommended that we not require entities to maintain records or account for prior disclosures for members who have ''disenrolled.''

Response: We agree with commenters who suggested we establish a specific period for which an individual may request an accounting. In the final rule, we provide that individuals have a right to an accounting of the applicable disclosures that have been made in the six-year period prior to a request for an accounting. We adopt this time frame to conform with the other documentation retention requirements in the rule. We also note that an individual may request, and a covered entity may then provide, an accounting of disclosures for a period of time less than six years from the date of the request. For example, an individual could request an accounting only of disclosures that occurred during the year prior to the request. In addition, we note that covered entities do not have to account for disclosures that occurred prior to the compliance date of this rule.

Comments: Commenters asked that we provide more time for entities to respond to requests for accounting. Suggestions ranged from 60 days to 90 days. Another writer suggested that entities be able to take up to three 30-day extensions from the original 30-day deadline. Commenters raised concerns about the proposed requirement that a covered health care provider or health plan act as soon as possible.

Response: We agree with concerns raised by commenters and in the final rule, covered entities are required to provide a requested accounting no later than 60 days after receipt of the request. We also provide for one 30 day extension if the covered entity is unable to provide the accounting within the standard time frame. We eliminate the requirement for a covered entity to act as soon as possible.

We recognize that circumstances may arise in which an individual will request an accounting on an expedited basis. We encourage covered entities to implement procedures for handling such requests. The time limitation is intended to be an outside deadline, rather than an expectation. We expect covered entities always to be attentive to the circumstances surrounding each request and to respond in an appropriate time frame.

Comment: A commenter asked that we provide an exemption for disclosures related to computer upgrades, when protected health information is disclosed to another entity solely for the purpose of establishing or checking a computer system.

Response: This activity falls within the definition of health care operations and is, therefore, excluded from the accounting requirement.

Section 164.530—Administrative Requirements

Section 164.530(a)—Designation of a Privacy Official and Contact Person

Comment: Many of the commenters on this topic objected to the cost of establishing a privacy official, including the need to hire additional staff, which might need to include a lawyer or other highly paid individual.

Response: We believe that designation of a privacy official is essential to ensure a central point of accountability within each covered entity for privacy-related issues. The privacy official is charged with developing and implementing the policies and procedures for the covered entity, as required throughout the regulation, and for compliance with the regulation generally. While the costs for these activities are part of the costs of compliance with this rule, not extra costs associated with the designation of a privacy official, we do anticipate that there will be some cost associated with this requirement. The privacy official role may be an additional responsibility given to an existing employee in the covered entity, such as an office manager in a small entity or an information officer or compliance official in a larger institution. Cost estimates for the privacy official are discussed in detail in the overall cost analysis.

Comment: A few commenters argued for more flexibility in meeting the requirement for accountability. One health care provider maintained that covered entities should be able to establish their own system of accountability. For example, most physician offices already have the patient protections incorporated in the proposed administrative requirements—the commenter urged that the regulation should explicitly promote the application of flexibility and scalability. A national physician association noted that, in small offices, in particular, responsibility for the policies and procedures should be allowed to be shared among several people. A major manufacturing corporation asserted that mandating a privacy official is unnecessary and that it would be preferable to ask for the development of policies that are designed to ensure that processes are maintained to assure compliance.

Response: We believe that a single focal point is needed to achieve the necessary accountability. At the same time, we recognize that covered entities are organized differently and have different information systems. We therefore do not prescribe who within a covered entity must serve as the privacy official, nor do we prohibit combining this function with other duties. Duties may be delegated and shared, so long as there is one point of accountability for the covered entity's policies and procedures and compliance with this regulation.

Comment: Some commenters echoed the proposal of a professional information management association that the regulation establish formal qualifications for the privacy official, suggesting that this should be a credentialed information management professional with specified minimum training standards. One commenter emphasized that the privacy official should be sufficiently high in management to have influence.

Response: While there may be some advantages to establishing formal qualifications, we concluded the disadvantages outweigh the advantages. Since the job of privacy official will differ substantially among organizations of varying size and function, specifying a single set of qualifications would sacrifice flexibility and scalability in implementation.

Comment: A few commenters suggested that we provide guidance on the tasks of the privacy official. One noted that this would reduce the burden on covered entities to clearly identify those tasks during the initial HIPAA implementation phase.

Response: The regulation itself outlines the tasks of the privacy official, by specifying the policies and procedures required, and otherwise explaining the duties of covered entities. Given the wide variation in the function and size of covered entities, providing further detail here would unnecessarily reduce flexibility for covered entities. We will, however, provide technical assistance in the form of guidance on the various provisions of the regulation before the compliance date.

Comment: Some comments expressed concern that the regulation would require a company with subsidiaries to appoint a privacy official within each subsidiary. Instead they argued that the corporate entity should have the option of designating a single corporate official rather than one at each subsidiary.

Response: In the final regulation, we give covered entities with multiple subsidiaries that meet the definition of covered entities under this rule the flexibility to designate whether such subsidiaries are each a separate covered entity or are together a single covered entity. (See § 164.504(b) for the rules requiring such designation.) If only one covered entity is designated for the subsidiaries, only one privacy officer is needed. Further, we do not prohibit the privacy official of one covered entity from serving as the privacy official of another covered entity, so long as all the requirements of this rule are met for each such covered entity.

Section 164.530(b)—Training

Comment: A few commenters felt that the proposed provision was too stringent, and that the content of the training program should be left to the reasonable discretion of the covered entity.

Response: We clarify that we do not prescribe the content of the required training; the nature of the training program is left to the discretion of the covered entity. The scenarios in the NPRM preamble of potential approaches to training for different sized covered entities were intended as examples of the flexibility and scalability of this requirement.

Comment: Most commenters on this provision asserted that recertification/retraining every three years is excessive, restrictive, and costly. Commenters felt that retraining intervals should be left to the discretion of the covered entity. Some commenters supported retraining only in the event of a material change. Some commenters supported the training requirement as specified in the NPRM.

Response: For the reasons cited by the commenters, we eliminate the triennial recertification requirements in the final rule. We also clarify that retraining is not required every three years. Retraining is only required in the case of material changes to the privacy policies and procedures of the covered entity.

Comment: Several commenters objected to the burden imposed by required signatures from employees after they are trained. Many commenters suggested that electronic signatures be accepted for various reasons. Some felt that it would be less costly than manually producing, processing, and retaining the hard copies of the forms. Some suggested sending out the notice to the personal workstation via email or some other electronic format and having staff reply via email. One commenter suggested that the covered entity might opt to give web based training instead of classroom or some other type. The commenter indicated that with web based training, the covered entity could record whether or not an employee had received his or her training through the use of a guest book or registration form on the web site. Thus, a physical signature should not be required.

Response: We agree that there are many appropriate mechanisms by which covered entities can implement their training programs, and therefore remove this requirement for signature. We establish only a general requirement that covered entities document compliance with the training requirement.

Comment: Some commenters were concerned that there was no proposed requirement for business associates to receive training and/or to train their employees. The commenters believed that if the business associate violated any privacy requirements, the covered entity would be held accountable. These commenters urged the Secretary to require periodic training for appropriate management personnel assigned outside of the component unit of the covered entity, including business associates. Other commenters felt that it would not be fair to require covered entities to impose training requirements on business associates.

Response: We do not have the statutory authority directly to require business associates to train their employees. We also believe it would be unnecessarily burdensome to require covered entities to monitor business associates' establishment of specific training requirements. Covered entities' responsibility for breaches of privacy by their business associates is described in §§ 164.504(e) and 164.530(f). If a covered entity believes that including a training requirement in one or more of its business associate contracts is an appropriate means of protecting the health information provided to the business associate, it is free to do so.

Comments: Many commenters argued that training, as well as all of the other administrative requirements, are too costly for covered entities and that small practices would not be able to bear the added costs. Commenters also suggested that HHS should provide training materials at little, or no, cost to the covered entity.

Response: For the final regulation, we make several changes to the proposed provisions. We believe that these changes address the issue of administrative cost and burden to the greatest extent possible, consistent with protecting the privacy of health information. In enforcing the privacy rule, we expect to provide general training materials. We also hope to work with professional associations and other groups that target classes of providers, plans and patients, in developing specialized material for these groups.

We note that, under long-standing legal principles, entities are generally responsible for the actions of their workforce. The requirement to train workforce members to implement the covered entity's privacy policies and procedures, and do such things as pass evidence of potential problems to those responsible, is in line with these principles. For example, the comments and our fact finding indicate that, today, many hospitals require their workforce members to sign a confidentiality agreement, and include confidentiality matters in their employee handbooks.

Section 164.530(c)—Safeguards

Comments: A few comments assert that the rule requires some institutions that do not have adequate resources to develop costly physical and technical safeguards without providing a funding mechanism to do so. Another comment said that the vague definitions of adequate and appropriate safeguards could be interpreted by HHS to require the purchase of new computer systems and reprogram many old ones. A few other comments suggested that the safeguards language was vague and asked for more specifics.

Response: We require covered entities to maintain safeguards adequate for their operations, but do not require that

specific technologies be used to do so. Safeguards need not be expensive or high-tech to be effective. Sometimes, it is an adequate safeguard to put a lock on a door and only give the keys to those who need access. As described in more detail in the preamble discussion of § 164.530, we do not require covered entities to guarantee the safety of protected health information against all assaults. This requirement is flexible and scalable to allow implementation of required safeguards at a reasonable cost.

Comments: A few commenters noted that once protected health information becomes non-electronic, by being printed for example, it escapes the protection of the safeguards in the proposed Security Rule. They asked if this safeguards requirement is intended to install similar security protections for non-electronic information.

Response: This provision is not intended to incorporate the provisions in the proposed Security regulation into this regulation, or to otherwise require application of those provisions to paper records.

Comments: Some commenters said that it was unclear what ''appropriate'' safeguards were required by the rule and who establishes the criteria for them. A few noted that the privacy safeguards were not exactly the same as the security safeguards, or that the ''other safeguards'' section was too vague to implement. They asked for more clarification of safeguards requirements and flexible solutions.

Response: In the preamble discussion of § 164.530, we provide examples of types of safeguards that can be appropriate to satisfy this requirement. Other sections of this regulation require specific safeguards for specific circumstances. The discussion of the requirements for ''minimum necessary'' uses and disclosures of protected health information includes related guidance for developing role-based access policies for a covered entity's workforce. The requirements for ''component entities'' include requirements for firewalls to prevent access by unauthorized persons. The proposed Security Rule included further details on what safeguards would be appropriate for electronic information systems. The flexibility and scalability of these rules allows covered entities to analyze their own needs and implement solutions appropriate for their own environment.

Comments: A few comments asked for a requirement for a firewall between a health care component and the rest of a larger organization as another appropriate safeguard.

Response: We agree, and have incorporated such a requirement in § 164.504.

Comments: One commenter agreed with the need for administrative, physical, and technical safeguards, but took issue with our specification of the type of documentation or proof that the covered entity is taking action to safeguard protected health information.

Response: This privacy rule does not require specific forms of proof for safeguards.

Comments: A few commenters asked that, for the requirement for a signed certification of training and the requirements for verification of identity, we consider the use of electronic signatures that meet the requirements in the proposed security regulation to meet the requirements of this rule.

Response: In this final rule, we drop the requirements for signed certifications of training. Signatures are required elsewhere in this regulation, for example, for a valid authorization. In the relevant sections we clarify that electronic signatures are sufficient provided they meet standards to be adopted under HIPAA. In addition, we do not intend to interfere with the application of the Electronic Signature in Global and National Commerce Act.

Comments: A few commenters requested that the privacy requirements for appropriate administrative, technical, and physical safeguards be considered to have been met if the requirements of the proposed Security Rule have been met. Others requested that the safeguards requirements of the final Privacy Rule mirror or be harmonized with the final Security Rule so they do not result in redundant or conflicting requirements.

Response: Unlike the proposed regulation, the final regulation covers all protected health information, not just information that had at some point been electronic. Thus, these commenters' assumption that the proposed Privacy Rule and the proposed Security Rule covered the same information is not the case, and taking the approach suggested by these comments would leave a significant number of health records unprotected. The safeguards required by this regulation are appropriate for both paper and electronic information. We will take care to ensure that the final Security Rule works in tandem with these requirements.

Comments: One commenter requested that the final privacy rule be published before the final Security Rule, recognizing that the privacy policies must be in place before the security technology used to implement them could be worked out. Another commenter asked that the final Security Rule be published immediately and not wait for an expected delay while privacy policies are worked out.

Response: Now that this final privacy rule has been published in a timely manner, the final Security Rule can be harmonized with it and published soon.

Comments: Several commenters echoed an association recommendation that, for those organizations that have implemented a computer based patient record that is compliant with the requirements of the proposed Security Rule, the minimum necessary rule should be considered to have been met by the implementation of role-based access controls.

Response: The privacy regulation applies to paper records to which the proposed Security Rule does not apply. Thus, taking the approach suggested by these comments would leave a significant number of health records unprotected. Further, since the final Security Rule is not yet published and the number of covered entities that have implemented this type of computer-based patient record systems is still small, we cannot make a blanket statement. We note that this regulation requires covered entities to develop role-based access rules, in order to implement the requirements for ''minimum necessary'' uses and disclosures of protected health information. Thus, this regulation provides a foundation for the type of electronic system to which these comments refer.

Section 164.530(d)—Complaints to the Covered Entity

Comment: Several commenters felt that some form of due process is needed when it comes to internal complaints. Specifically, they wanted to be assured that the covered entity actually hears the complaints made by the individual and that the covered entity resolves the complaint within a reasonable time frame. Without due process the commenters felt that the internal complaint process is open ended. Some commenters wanted the final rule to include an appeals process for individuals if a covered entity's determination in regards to the complaint is unfavorable to the individual.

Response: We do not require covered entities to implement any particular due process or appeals process for complaints, because we are concerned about the burden this could impose on covered entities. We provide individuals with an alternative to take their complaints to the Secretary. We believe that this provides incentives for

covered entities to implement a complaint process that resolves complaints to individuals' satisfaction.

Comment: Some commenters felt that the individual making the complaint should exhaust all other avenues to resolve their issues before filing a complaint with the Secretary. A number of commenters felt that any complaint being filed with the Secretary should include documentation of the reviews done by the covered entity.

Response: We reject these suggestions, for two reasons. First, we want to avoid establishing particular process requirements for covered entities' complaint programs. Also, this rule does not require the covered entity to share any information with the complainant, only to document the receipt of the complaint and the resolution, if any. Therefore, we cannot expect the complainant to have this information available to submit to the Secretary. Second, we believe the individual making the complaint should have the right to share the complaint with the Secretary at any point in time. This approach is consistent with existing civil rights enforcement programs for which the Department is responsible. Based on that experience, we believe that most complaints will come first to covered entities for disposition.

Comment: Some commenters wanted the Department to prescribe a minimum amount of time before the covered entity could dispose of the complaints. They felt that storing these complaints indefinitely would be cumbersome and expensive.

Response: We agree, and in the final rule require covered entities to keep all items that must be documented, including complaints, for at least six years from the date of creation.

Comments: Some commenters objected to the need for covered entities to have at least one employee, if not more, to deal with complaints. They felt that this would be costly and is redundant in light of the designation of a contact person to receive complaints.

Response: We do not require assignment of dedicated staff to handle complaints. The covered entity can determine staffing based on its needs and business practices. We believe that consumers need one clear point of contact for complaints, in order that this provision effectively inform consumers how to lodge complaints and so that the compliant will get to someone who knows how to respond. The contact person (or office) is for receipt of complaints, but need not handle the complaints.

Section 164.530(e)—Sanctions

Comment: Commenters argued that most covered entities already have strict sanctions in place for violations of a patient's privacy, either due to current laws, contractual obligations, or good operating practices. Requiring covered entities to create a formal sanctioning process would be superfluous.

Response: We believe it is important for the covered entity to have these sanction policies and procedures documented so that employees are aware of what actions are prohibited and punishable. For entities that already have sanctions policies in place, it should not be problematic to document those policies. We do not define the particular sanctions that covered entities must impose.

Comment: Several commenters agreed that training should be provided and expectations should be clear so that individuals are not sanctioned for doing things that they did not know were wrong or inappropriate. A good faith exception should be included in the final rule to protect these individuals.

Response: We agree that employees should be trained to understand the covered entity's expectations and understand the consequences of any violation. This is why we are requiring each covered entity to train its workforce. However, we disagree that a good faith exception is explicitly needed in the final rule. We leave the details of sanctions policies to the discretion of the covered entity. We believe it is more appropriate to leave this judgment to the covered entity that will be familiar with the circumstances of the violation, rather than to specify such requirements in the regulation.

Comment: Some commenters felt that the sanctions need to reach business partners as well, not just employees of the covered entities. These commenters felt all violators should be sanctioned, including government officials and agencies.

Response: All members of a covered entity's workforce are subject to sanctions for violations, including government officials who are part of a covered entity's workforce. Requirements for addressing privacy violations by business associates are discussed in §§ 164.504(e) and 164.530(f).

Comments: Many commenters appreciated the flexibility left to the covered entities to determine sanctions. However, some were concerned that the covered entity would need to predict each type of violation and the associated sanction. They argue that, if the Department could not determine this in the NPRM, then the covered entities should be allowed to come up with sanctions as appropriate at the time of the violation. Some commenters wanted a better explanation and understanding of what HHS' expectation is of when is it appropriate to apply sanctions. Some commenters felt that the sanctioning requirement is nebulous and requires independent judgment of compliance; as a result it is hard to enforce. Offending individuals may use the vagueness of the standard as an defense.

Response: We agree with the commenters that argue that covered entities should be allowed to determine the specific sanctions as appropriate at the time of the violation. We believe it is more appropriate to leave this judgment to the covered entity, because the covered entity will be familiar with the circumstances of the violation and the best way to improve compliance.

Comment: A commenter felt that the self-imposition of this requirement is an inadequate protection, as there is an inherent conflict of interest when an entity must sanction one of its own.

Response: We believe it is in the covered entity's best interests to appropriately sanction those individuals who do not follow the outlined policies and procedures. Allowing violations to go unpunished may lead bigger problems later, and result in complaints being registered with the Department by aggrieved parties and/or an enforcement action.

Comment: This provision should cover all violations, not just repeat violations.

Response: We do not limit this requirement to repeat offenses.

Section 164.530(f)—Duty To Mitigate

Comments: A few commenters felt that any duty to mitigate would be onerous, especially for small entities. One commenter supported an affirmative duty to mitigate for employees of the covered entity, as long as there is no prescribed mitigation policy. One commenter stated that a requirement for mitigation is unnecessary because any prudent entity would do it.

Some practitioner organizations as well as a health plan, expressed concern about the obligation to mitigate in the context of the business associate relationship. Arguing that it is unnecessary for the regulation to explicitly extend the duty to mitigate to business associates, commenters noted that: Any prudent entity would discipline a vendor or employee that violates a regulation; that the matter is best left to the terms of the contract, and that it is difficult and expensive for a

business associate to have a separate set of procedures on mitigation for each client/provider. One commenter suggested that the federal government should fund the monitoring needed to administer the requirement.

Response: Eliminating the requirement to mitigate harm would undermine the purposes of this rule by reducing covered entities' accountability to their patients for failure to protect their confidential data. To minimize burden, we do not prescribe what mitigation policies and procedures must be implemented. We require only that the covered entity mitigate harm. We also assume that violations will be rare, and so the duty to mitigate harm will rarely be triggered. To the extent a covered entity already has methods for mitigating harm, this rule will not pose significant burden, since we don't require the covered entity to follow any prescribed method or set of rules.

We also modify the NPRM to impose the duty to mitigate only where the covered entity has actual knowledge of harm. Further reducing burden, the rule requires mitigation ''to the extent practicable.'' It does not require the covered entity to eliminate the harm unless that is practicable. For example, if protected health information is advertently provided to a third party without authorization in a domestic abuse situation, the covered entity would be expected to promptly contact the patient as well as appropriate authorities and apprize them of the potential danger.

The harm to the individual is the same, whether the privacy breach was caused by a member of the covered entity's workforce, or by a contractor. We believe the cost of this requirement to be minimal for covered entities that engage in prudent business practices for exchanging protected health information with their business associates.

Comment: A few commenters noted that it is difficult to determine whether a violation has resulted in a deleterious effect, especially as the entity cannot know all places to which information has gone and uses that have been made of it. Consequently, there should be a duty to mitigate even if a deleterious effect cannot be shown, because the individual has no other redress.

Response: As noted above, this provision only applies if the covered entity has actual knowledge of the harm, and requires mitigation ''to the extent practicable.'' The covered entity is expected to take reasonable steps based on knowledge of where the information has been disclosed, how it might be used to cause harm to the patient or another individual, and what steps can actually have a mitigating effect in that specific situation.

Comments: Commenters stated that the language of the regulation was in some places vague and imprecise thus providing covered entities with insufficient guidance and allowing variation in interpretation. Commenters also noted that this could result in inconsistency in implementation as well as permitting such inconsistency to be used as a defense by an offending entity. Particular language for which at least one commenter requested clarification included ''reasonable steps'' and what is entailed in the duty to mitigate.

Response: We considered ways in which we might increase specificity, including defining ''to the extent practicable'' and ''reasonable steps'' and relating the mitigating action to the deleterious impact. While this approach could remove from the covered entity the burden of decision-making about actions that need to be taken, we believe that other factors outweighed this potential benefit. Not only would there be a loss of desirable flexibility in implementation, but it would not be possible to define ''to the extent practicable'' in a way that makes sense for all types of covered entities. We believe that allowing flexibility and judgment by those familiar with the circumstances to dictate the approach is the best approach to mitigating harm.

Section 164.530(g)—Refraining From Intimidating or Retaliatory Acts

Comment: Several commenters stated that the regulation should prohibit covered entities from engaging in intimidating or retaliatory acts against any person, not just against the ''individual,'' as proposed. They suggested adding ''or other person or entity'' after ''any individual.''

Response: We agree, and allow any person to file a compliant with the Secretary. ''Person'' is not limited to natural persons, but includes any type of organization, association or group such as other covered entities, health oversight agencies and advocacy groups.

Comment: A few commenters suggested deleting this provision in its entirety. One commenter indicated that the whistleblower and retaliation provisions could be inappropriately used against a hospital and that the whistleblower's ability to report numerous violations will result in a dangerous expansion of liability. Another commenter stated that covered entities could not take action against an employee who had violated the employer's privacy provisions if this employee files a complaint with the Secretary.

Several commenters suggested deleting ''in any manner'' and ''or opposing any act or practice made unlawful by this subpart'' in § 164.522(d)(4). The commenters indicated that, as proposed, the rule would make it difficult to enforce compliance within the workforce. One commenter stated that the proposed 164.522(d)(4) ''is extremely broad and may allow an employee to reveal protected health information to fellow employees, the media and others (e.g., an employee may show a medical record to a friend or relative before filing a complaint with the Department). This commenter further stated that covered entities will ''absolutely be prevented from prohibiting such conduct.'' One commenter suggested adding that a covered entity may take disciplinary action against any member of its work force or any business partner who uses or discloses individually identifiable health information in violation of this subpart in any manner other than through the processes set forth in the regulation.

Response: To respond to these comments, we make several changes to the proposed provision.

First, where the activity does not involve the filing of a complaint under § 160.306 of this part or participation in an investigation or proceeding initiated by the government under the rule, we delete the phrase ''in any manner'' and add a requirement that the individual's opposition to ''any act or practice'' made unlawful by this subpart be in good faith, and that the expression of that opposition must be reasonable. Second, we add a requirement that the individual's opposition to ''any act or practice'' made unlawful by this subpart must not involve a disclosure of protected health information that is in violation of this subpart. Thus, the employee who discloses protected health information to the media or friends is not protected. In providing interpretations of the retaliation provision, we will consider existing interpretations of similar provisions such as the guidance issued by EEOC in this regard.

Section 164.530(h)—Waiver of Rights

There are no comments directly about this section because it was not included in the proposed rule.

Section 164.530(i)—Policies and Procedures and § 164.530(j)—Documentation Requirements

Comments: Many of the comments to this provision addressed the costs and

complexity of the regulation as a whole, not the additional costs of documenting policies and procedures per se. Some did, either implicitly or explicitly, object to the need to develop and document policies and procedures as creating excessive administrative burden. Many of these commenters also asserted that there is a contradiction between the administrative burden of this provision and one of the statutory purposes of this section of the HIPAA to reduce costs through administrative simplification. Suggested alternatives were generally reliance on existing regulations and ethical standards, or on current business practices.

Response: A specific discussion of cost and burden is found in the Regulatory Impact Analysis of this final rule.

We do not believe there is a contradiction between the administrative costs of this provision and of the goal of administrative simplification. In the Administrative Simplification provisions of the HIPAA, Congress combined a mandate to facilitate the efficiencies and cost savings for the health care industry that the increasing use of electronic technology affords, with a mandate to improve privacy and confidentiality protections. Congress recognized, and we agree, that the benefits of electronic commerce can also cause increased vulnerability to inappropriate access and use of medical information, and so must be balanced with increased privacy protections. By including the mandate for privacy standards in section 264 of the HIPAA, Congress determined that existing regulations and ethical standards, and current business practices were insufficient to provide the necessary protections.

Congress mandated that the total benefits associated with administrative simplification must outweigh its costs, including the costs of implementing the privacy regulation. We are well within this mandate.

Comments: Several commenters suggested that the documentation requirements not be established as a standard under the regulation, because standards are subject to penalties. They recommend we delete the documentation standards and instead provide specific guidance and technical assistance. Several commenters objected to the suggestion in the NPRM that professional associations assist their members by developing appropriate policies for their membership. Several commentators representing professional associations believed this to be an onerous and costly burden for the associations, and suggested instead that we develop specific models which might require only minor modification. Some of these same associations were also concerned about liability issues in developing such guidelines. One commenter argued that sample forms, procedures, and policies should be provided as part of the Final Rule, so that practitioners would not be overburdened in meeting the demands of the regulations. They urged us to apply this provision only to larger entities.

Response: The purpose of requiring covered entities to develop policies and procedures for implementing this regulation is to ensure that important decisions affecting individuals' rights and privacy interests are made thoughtfully, not on an ad hoc basis. The purpose of requiring covered entities to maintain written documentation of these policies is to facilitate workforce training, and to facilitate creation of the required notice of information practices. We further believe that requiring written documentation of key decisions about privacy will enhance accountability, both within the covered entity and to the Department, for compliance with this regulation.

We do not include more specific guidance on the content of the required policies and procedures because of the vast difference in the size of covered entities and types of covered entities' businesses. We believe that covered entities should have the flexibility to design the policies and procedures best suited to their business and information practices. We do not exempt smaller entities, because the privacy of their patients is no less important than the privacy of individuals who seek care from large providers. Rather, to address this concern we ensure that the requirements of the rule are flexible so that smaller covered entities need not follow detailed rules that might be appropriate for larger entities with complex information systems.

We understand that smaller covered entities may require some assistance, and intend to provide such technical assistance after publication of this rule. We hope to work with professional associations and other groups that target classes of providers, plans and patients, in developing specialized material for these groups. Our discussions with several such organizations indicate their intent to work on various aspects of model documentation, including forms. Because the associations' comments regarding concerns about liability did not provide sufficient details, we cannot address them here.

Comment: Many commenters discussed the need for a recognition of scalability of the policies and procedures of an entity based on size, capabilities, and needs of the participants. It was noted that the actual language of the draft regulations under § 164.520 did not address scalability, and suggested that some scalability standard be formally incorporated into the regulatory language and not rely solely on the NPRM introductory commentary.

Response: In § 164.530(i)(1) of the final rule, we specify that we require covered entities to implement policies and procedures that take into account the size of the covered entity and the types of activities that relate to protected health information undertaken by the covered entity.

Comment: One commenter objected to our proposal to allow covered entities to make uses or disclosures not permitted by their current notice if a compelling reason exists to make the use or disclosure and the entity documents the reasons and changes its policies within 30 days of the use or disclosure. The commenter argued that the subjective language of the regulation might give entities the ability to engage in post hoc justifications for violations of their own information practices and policies. The commenter suggested that there should be an objective standard for reviewing the covered entity's reasons before allowing the covered entity to amend its policies.

Response: We eliminate this provision from the final rule. The final rule requires each covered entity to include in its notice of information practices a statement of all permitted uses under this rule, not just those in which the covered entity actually engages in at the time of that notice.

Comment: Some commenters expressed concern that the required retention period in the NPRM applied to the retention of medical records.

Response: The retention requirement of this regulation only applies to the documentation required by the rule, for example, keeping a record of accounting for disclosures or copies of policies and procedures. It does not apply to medical records.

Comments: Comments on the six year retention period were mixed. Some commenters endorsed the six-year retention period for maintaining documentation. One of the comments stated this retention period would assist physicians legally. Other commenters believed that the retention period would be an undue burden. One commenter noted that most State Board of Pharmacy regulations require

pharmacies to keep records for two years, so the six year retention period would triple document retention costs.

Response: We established the retention period at six years because this is the statute of limitations for the civil monetary penalties. This rule does not apply to all pharmacy records, but only to the documentation required by this rule.

Section 164.530(k)—Group Health Plans

There were no comments directly about this section because it was not included in the proposed rule.

Section 164.532—Transition Provisions

Comment: Commenters urged the Department to clarify whether the ''reach of the transition requirement'' is limited to a particular time frame, to the provider's activities in a particular job, or work for a particular employer. For example, one commenter questioned how long a nurse is a covered entity after she moves from a job reviewing files with protected health information to an administrative job that does not handle protected health information; or whether an occupational health nurse who used to transmit first reports of injury to her company's workers' compensation carrier last year but no longer does so this year because of a carrier change still is a covered entity.

Response: Because this comment addresses a question of enforcement, we will address it in the enforcement regulation.

Comment: Several commenters sought clarification as to the application of the privacy rule to research already begun prior to the effective date or compliance date of the final rule. These commenters argued that applying the privacy rule to research already begun prior the rule's effective date would substantially overburden IRBs and that the resulting research interruptions could harm participants and threaten the reliability and validity of conclusions based upon clinical trial data. The commenters recommended that the rule grandfather in any ongoing research that has been approved by and is under the supervision of an IRB.

Response: We generally agree with the concerns raised by commenters. In the final rule, we have provided that covered entities may rely upon consents, authorizations, or other express legal permissions obtained from an individual for a specific research project that includes the treatment of individuals to use or disclose protected health information the covered entity obtained before or after the applicable compliance date of this rule as long as certain requirements are met. These consents, authorizations, or other express legal permissions may specifically permit a use or disclosure of individually identifiable health information for purposes of the project or be a general consent of the individual to participate in the project. A covered entity may use or disclose protected health information it created or received before or after the applicable compliance date of this rule for purposes of the project provided that the covered entity complies with all limitations expressed in the consent, authorization, or permission.

In regard to research projects that include the treatment of individuals, such as clinical trials, covered entities engaged in these projects will have obtained at least an informed consent from the individual to participate in the project. In some cases, the researcher may also have obtained a consent, authorization, or other express legal permission to use or disclose individually identifiable health information in a specific manner. To avoid disrupting ongoing research and because the participants have already agreed to participate in the project (which expressly permits or implies the use or disclosure of their protected health information), we have grandfathered in these consents, authorizations, and other express legal permissions.

It is unlikely that a research project that includes the treatment of individuals could proceed under the Common Rule with a waiver of informed consent. However, to the extent such a waiver has been granted, we believe individuals participating in the project should be able to determine how their protected health information is used or disclosed. Therefore, we require researchers engaged in research projects that include the treatment of individuals who obtained an IRB waiver of informed consent under the Common Rule to obtain an authorization or a waiver of such authorization from an IRB or a privacy board under § 164.512(i) of this rule.

If a covered entity obtained a consent, authorization, or other express legal permission from the individual who is the subject of the research, it would be able to rely upon that consent, authorization, or permission, consistent with any limitations it expressed, to use or disclose the protected health information it created or received prior to or after the compliance date of this regulation. If a covered entity wishes to use or disclose protected health information but no such consent, authorization, or permission exists, it must obtain an authorization pursuant to § 164.508 or obtain a waiver of authorization under § 164.512(i). To the extent such a project is ongoing and the researchers are unable to locate the individuals whose protected health information they are using or disclosing, we believe the IRB or privacy board under the criteria set forth in § 164.512(i) will be able to take that circumstance into account when conducting its review. In most instances, we believe this type of research will be able to obtain a waiver of authorization and be able to continue uninterrupted.

Comment: Several comments raised questions about the application of the rule to individually identifiable information created prior to (1) the effective date of the rule, and (2) the compliance dates of the rule. One commenter suggested that the rule should apply only to information gathered after the effective date of the final rule. A drug manufacturer asked what would be the effect of the rule on research on records compiled before the effective date of the rule.

Response: We disagree with the commenter's suggestion. The requirements of this regulation apply to all protected health information held by a covered entity, regardless of when or how the covered entity obtained the information. Congress required us to adopted privacy standards that apply to individually identifiable health information. While it limited the compliance date for health plans, covered health care providers, and healthcare clearinghouses, it did not provide similar limiting language with regard to individually identifiable health information. Therefore, uses and disclosures of protected health information made by a covered entity after the compliance date of this regulation must meet the requirements of these rules. Uses or disclosures of individually identifiable health information made prior to the compliance date are not affected; covered entities will not be sanctioned under this rule based on past uses or disclosures that are inconsistent with this regulation.

Consistent with the definition of individually identifiable health information in HIPAA, of which protected health information is a subset, we do not distinguish between protected health information in research records and protected health information in other records. Thus, a covered entity's research records are subject to this regulation to the extent they contain protected health information.

Section 164.534—Effective Date and Compliance Date

Section 1175(b)(1)(A) of the Act requires all covered entities other than small health plans to comply with a standard or implementation specification ''not later than 24 months after the date on which an initial standard or implementation specification is adopted or established''; section 1175(b)(1)(B) provides that small health plans must comply not later than 36 months after that date. The proposed rule provided, at proposed § 164.524 (which was titled ''Effective date''), that a covered entity was required to be in compliance with the proposed subpart E not later than 24 months following the effective date of the rule, except that small health plans were required to be in compliance not later than 36 months following the effective date of the rule.

The final rules retain these dates in the text of Subpart E, but denominate them as ''compliance dates,'' to distinguish the statutory dates from the date on which the rules become effective. The effective date of the final rules is 60 days following publication in the **Federal Register.**

Meaning of Effective Date

Comment: A number of commenters expressed confusion about the difference between the effective date of the rule and the effective date on which compliance was required (the statutory compliance dates set out at section 1175(b)(1), summarized above).

Response: The Department agrees that the title of proposed § 164.524 was confusing. Similar comments were received on the Transactions Rule. Those comments were addressed by treating the ''effective date'' of the rule as the date on which adoption takes effect (the ''Effective Date'' heading at the beginning of the preamble), while the dates provided for by section 1175(b)(1) of the statute were denominated as ''compliance dates.'' These changes are reflected in the definition of ''compliance date'' in § 160.103 below (initially published as part of the Transactions Rule) and are also reflected at § 164.524 below. Section 164.524 below has also been reorganized to follow the organization of the analogous provisions of the Transactions Rule. The underlying policy, however, remains as proposed.

Extend the Compliance Date

Comment: Some commenters recommended that the compliance date be extended. A number of comments objected that the time frame for compliance with the proposed standards is unrealistically short. It was pointed out that providers and others would have to do the following, among other things, prior to the applicable compliance date: assess their current systems and departments, determine which state laws were preempted and which were not, update and reprogram computer systems, train workers, create and implement the required privacy policies and procedures, and create or update contracts with business partners. One comment also noted that the task of coming into compliance during the same time period with the other regulations being issued under HIPAA would further complicate the task. These comments generally supported an extension of the compliance dates by one or more years. Other comments supported extending the compliance dates on the ground that the complexity of the tasks involved in implementing the regulation would be a heavy financial burden for providers and others, and that they should be given more time to comply, in order to spread the associated capital and workforce costs over a longer period. It was also suggested that there be provision for granting extensions of the compliance date, based on some criteria, such as a good faith effort to comply or that the compliance dates be extended to two years following completion of a ''state-by-state preemption analysis'' by the Department.

Response: The Secretary acknowledges that covered entities will have to make changes to their policies and procedures during the period between the effective date of the rules below and the applicable compliance dates. The delayed compliance dates which the statute provides for constitute a recognition of the fact changes will be required and are intended to permit covered entities to manage and implement these changes in an orderly fashion. However, because the time frames for compliance with the initial standards are established by statute, the Secretary has no discretion to extend them: Compliance is statutorily required ''not later than'' the applicable compliance date. Nor do we believe that it would be advisable to accomplish this result by delaying the effective date of the final rules beyond 60 days. Since the Transactions Rule is now in effect, it is imperative to bring the privacy protections afforded by the rules below into effect as soon as possible. Retaining the delayed effective date of 60 days, as originally contemplated, will minimize the gap between transactions covered by those rules and not also afforded protection under the rules below.

Phase-in Requirements

Comment: Several comments suggested that the privacy standards be phased in gradually, to ease the manpower and cost burdens of compliance. A couple of equipment manufacturing groups suggested that updating of various types of equipment would be necessary for compliance purposes, and suggested a phased approach to this—for example, an initial phase consisting of preparation of policies, plans, and risk assessments, a second phase consisting of bringing new equipment into compliance, and a final phase consisting of bringing existing equipment into compliance.

Response: As noted in the preceding response, section 1175(b)(1) does not allow the Secretary discretion to change the time frame within which compliance must be achieved. Congress appears to have intended the phasing in of compliance to occur during the two-year compliance period, not thereafter.

Compliance Gap Vis-à-Vis State Laws and Small Health Plans

Comment: Several comments stated that, as drafted, the preemption provisions would be effective as of the rule's effective date (*i.e.,* 60 days following publication), even though covered entities would not be required to comply with the rules for at least another two years. According to these comments, the ''preempted'' state laws would not be in effect in the interim, so that the actual privacy protection would decrease during that period. A couple of comments also expressed concern about how the preemption provisions would work, given the one-year difference in applicable compliance dates for small health plans and other covered entities. A state medical society pointed out that this gap would also be very troublesome for providers who deal with both ''small health plans'' and other health plans. One comment asked what entities that decided to come into compliance early would have to do with respect to conflicting state laws and suggested that, since all parties ''need to know with confidence which laws govern at the moment, * * * [t]here should be uniform effective dates.''

Response: We agree that clarification is needed with respect to the applicability of state laws in the interim between the effective date and the compliance dates. What the comments summarized above appeared to assume is that the preemption provisions of section 1178 operate to broadly and generally invalidate any state law that comes within their ambit. We do not agree that this is the effect of section

1178. Rather, what section 1178 does—where it acts to preempt—is to preempt the state law in question with respect to the actions of covered entities to which the state law applies. Thus, if a provision of state law is preempted by section 1178, covered entities within that state to which the state law applies do not have to comply with it, and must instead comply with the contrary federal standard, requirement, or implementation specification. However, as compliance with the contrary federal standard, requirement, or implementation specification is not required until the applicable compliance date, we do not view the state law in question as meeting the test of being ''contrary.'' That is, since compliance with the federal standard, requirement, or implementation standard is not required prior to the applicable compliance date, it is possible for covered entities to comply with the state law in question. See § 160.202 (definition of ''contrary''). Thus, since the state law is not ''contrary'' to an applicable federal standard, requirement, or implementation specification in the period before which compliance is required, it is not preempted.

Several implications of this analysis should be spelled out. First, one conclusion that flows from this analysis is that preemption is specific to covered entities and does not represent a general invalidation of state law, as suggested by many commenters. Second, because preemption is covered entity-specific, preemption will occur at different times for small health plans than it will occur for all other covered entities. That is, the preemption of a given state law for a covered entity, such as a provider, that is covered by the 24-month compliance date of section 1175(b)(1)(A) will occur 12 months earlier than the preemption of the same state law for a small health plan that is covered by the 36-month compliance date of section 1175(b)(1)(B). Third, the preemption occurs only for covered entities; a state law that is preempted under section 1178(a)(1) would not be preempted for persons and entities to which it applies who are not covered entities. Thus, to the extent covered entities or non-covered entities follow the federal standards on a voluntary basis (*i.e.,* the covered entity prior to the applicable compliance date, the non-covered entity at any time), the state law in question will not be preempted for them.

Small Health Plans

Comment: Several comments, pointing to the ''Small Business'' discussion in the preamble to the proposed rules, applauded the decision to extend the compliance date to three years for small businesses. It was requested that the final rules clarify that the three year compliance date applies to small doctors offices and other small entities, as well as to small health plans.

Response: We recognize that our discussion in the preamble to the proposed rules may have suggested that more covered entities came within the 36 month compliance date than is in fact the case. Again, this is an area in which we are limited by statute. Under section 1175(b) of the Act, only small health plans have three years to come into compliance with the standards below. Thus, other ''small businesses'' that are covered entities must comply by the two-year compliance date.

Coordination With the Security Standard

Comment: Several comments suggested that the security standard be issued either with or after the privacy standards. It was argued that both sets of standards deal with protecting health information and will require extensive personnel training and revisions to business practices, so that coordinating them would make sense. An equipment manufacturers group also pointed out that it would be logical for covered entities and their business partners to know what privacy policies are required in purchasing security systems, and that ''the policies on privacy are implemented through the security standards rather than having already finalized security standards drive policy.''

Response: We agree with these comments, and are making every effort to coordinate the final security standards with the privacy standards below. The privacy standards below are being published ahead of the security standards, which is also responsive to the stated concerns.

Prospective Application

Comment: Several comments raised questions about the application of the rule to individually identifiable information created prior to (1) the effective date of the rule, and (2) the compliance dates of the rule. One provider group suggested that the rule should apply only to information gathered after the effective date of the final rule. A drug manufacturer asked what would be the effect of the rule on research on records compiled before the effective date of the rule.

Response: These comments are addressed in connection with the discussion of § 164.532 above.

Impact Analyses

Cost/Benefit Analysis

Comment: Many commenters made general statements to the effect that the cost estimates for implementing the provisions of the proposed regulation were incomplete or greatly understated.

Response: The proposal, including the cost analysis, is, in effect, a first draft. The purpose of the proposal was to solicit public comment and to use those comments to refine the final regulation. As a result of the public comment, the Department has significantly refined our initial cost estimates for implementing this regulation. The cost analysis below reflects a much more complete analysis of the major components of the regulation than was presented in the proposal.

Comment: Numerous commenters noted that significant areas of potential cost had not been estimated and that if they were estimated, they would greatly increase the total cost of the regulation. Potential cost areas identified by various respondents as omitted from the analyses include the minimum disclosure requirements; the requisite monitoring by covered entities of business partners with whom they share private health information; creation of de-identified information; internal complaint processes; sanctions and enforcement; the designation of a privacy official and creation of a privacy board; new requirements for research/optional disclosures; and future litigation costs.

Response: We noted in the proposed rule that we did not have data from which to estimate the costs of many provisions, and solicited comments providing such data. The final analysis below reflects the best estimate possible for these areas, based on the information available. The data and the underlying assumptions are explained in the cost analysis section below.

Comment: A number of comments suggested that the final regulation be delayed until more thorough analyses could be undertaken and completed. One commenter stated that the Department should refrain from implementing the regulation until a more realistic assessment of costs could be made and include local governments in the process. Similarly, a commenter requested that the Department assemble an outside panel of health industry experts, including systems analysts, legal counsel, and management consultants to develop stronger estimates.

Response: The Department has engaged in extensive research, data collection and fact-finding to improve

the quality of its economic analysis. This has included comments from and discussions with the kinds of experts one commenter suggested. The estimates represent a reasonable assessment of the policies proposed.

Comment: Several commenters indicated that the proposed regulation would impose significant new costs on providers' practices. Furthermore, they believe that it runs counter to the explicit statutory intent of HIPAA's Administrative Simplification provisions which require that ''any standard adopted * * * shall be consistent with the objective of reducing the administrative costs of providing and paying for health care.''

Response: As the Department explained in the Transactions Rule, this provision applies to the administrative simplification regulations of HIPAA in the aggregate. The Transactions Rule is estimated to save the health care system $29.9 billion in nominal dollars over ten years. Other regulations published pursuant to the administrative simplification authority in HIPAA, including the privacy regulation, will result in costs, but these costs are within the statutory directive so long as they do not exceed the $29.9 billion in estimated savings. Furthermore, as explained in the Transactions Rule, and the preamble to this rule, assuring privacy is essential to sustaining many of the advances that computers will provide. If people do not have confidence that their medical privacy will be protected, they will be much less likely to allow their records to be used for any purpose or might even avoid obtaining necessary medical care.

Comment: Several commenters criticized the omission of aggregate, quantifiable benefit estimates in the proposed rule. Some respondents argued that the analysis in the proposed rule used ''de minimis'' cost estimates to argue only that benefits would certainly exceed such a low barrier. These commenters further characterized the benefits analysis in the Notice of Proposed Rulemaking as ''hand waving'' used to divert attention from the fact that no real cost-benefit comparison is presented. Another commenter stated that the benefit estimates rely heavily on anecdotal and unsubstantiated inferences. This respondent believes that the benefit estimates are based on postulated, but largely unsubstantiated causal linkages between increased privacy and earlier diagnosis and medical treatment.

Response: The benefits of privacy are diffused and intangible but real. Medical privacy is not a good people buy or sell in a market; therefore, it is very difficult to quantify. The benefits discussion in the proposal reflects this difficulty. The examples presented in the proposal were meant to be illustrative of the benefits based on a few areas of medicine where some relevant data was available. Unfortunately, no commenters provided either a better methodological approach or better data for assessing the overall benefits of privacy. Therefore, we believe the analysis in the proposal represents a valid illustration of the benefits of privacy, and we do not believe it is feasible to provide an overall dollar estimate of the benefits of privacy in the aggregate.

Comment: One commenter criticized the benefit analysis as being incomplete because it did not consider the potential cost of new treatments that might be engendered by increased confidence in medical privacy resulting from the regulation.

Response: There is no data or model to reliably assess such long-term behavioral and scientific changes, nor to determine what portion of the increasingly rapid evolution of new improved treatments might stem from improved privacy protections. Moreover, to be complete, such analysis would have to include the savings that might be realized from earlier detection and treatment. It is not possible at this time to project the magnitude or even the direction of the net effects of the response to privacy that the commenter suggests.

Scope of the Regulation

Comment: Numerous commenters noted the potential cost and burden of keeping track in medical records of information which had been transmitted electronically, which would be subject to the rule, as opposed to information that had only been maintained in paper form.

Response: This argument was found to have considerable merit and was one of the reasons that the Department concluded that the final regulation should apply to all medical records maintained by covered entities, including information that had never been transmitted electronically. The costs analysis below reflects the change in scope.

Notice Requirements

Comment: Several commenters expressed their belief that the administrative and cost burdens associated with the notice requirements were understated in the proposed rule. While some respondents took issue with the policy development cost estimates associated with the notice, more were focused on its projected implementation and production costs. For example, one respondent stated that determining ''first service'' would be an onerous task for many small practices, and that provider staff will now have to manually review each patient's chart or access a computer system to determine whether the patient has been seen since implementation of the rule.

Response: The policy in the final rule has been changed to make the privacy policy notice to patients less burdensome. Providers will be able to distribute the notice when a patient is seen and will not have to distribute it to a patient more than once, unless substantive changes are made in the notice. This change will significantly reduce the cost of distributing the privacy notices.

Comment: Some commenters also took issue with the methodology used to calculate the cost estimates for notices. These respondents believe that the survey data used in the proposed rule to estimate the costs (*i.e.,* ''encounters,'' ''patients,'' and ''episodes'' per year) are very different concepts that, when used together, render the purported total meaningless. Commenters further stated that they can verify the estimate of 543 million patients cited as being seen at least once every five years.

Response: In the course of receiving treatment, a patient may go to a number of medical organizations. For example, a person might see a doctor in a physician's office, be admitted to a hospital, and later go to a pharmacy for medication. Each time a person ''encounters'' a facility, a medical record may be started or additions made to an existing record. The concept in the proposal was to identify the number of record sets that a person might have for purposes of estimating notice and copying costs. For example, whether a person made one or ten visits in the course of a year to a specific doctor would, for our purposes, be one record set because in each visit the doctor would most likely be adding information to an existing medical record. The comments demonstrated that we had not explained the concept well. As explained below we modified the concept to more effectively measure the number of record sets that exist and explain it more clearly.

Comment: Several commenters criticized the lack of supporting evidence for the cost estimates of notice development and dissemination. Another opinion voiced in the comments is that the estimated cost for plans of $0.75 per insured person is so low that it may cover postage, but it

cannot include labor and capital usage costs.

Response: Based on comments and additional fact finding, the Department was able to gain a better understanding of how covered entities would develop policies and disseminate information. The cost analysis below explains more fully how we derived the final cost estimates for these areas.

Comment: A commenter noted that privacy policy costs assume that national associations will develop privacy policies for members but HHS analysis does not account for the cost to the national associations. A provider cost range of $300–$3,000 is without justification and seems low.

Response: The cost to the national associations was included in the proposal estimates, and it is included in the final analysis (see below).

Comment: A commenter states that the notice costs discussion mixes the terms ''patients'', ''encounters'' and ''episodes'' and 397 million encounter estimate is unclear.

Response: A clearer explanation of the concepts employed in this analysis is provided below.

Systems Compliance Costs

Comment: Numerous commenters questioned the methodology used to estimate the systems compliance cost and stated that the ensuing cost estimates were grossly understated. Some stated that the regulation will impose significant information technology costs to comply with requirement to account for disclosures, additional costs for hiring new personnel to develop privacy policies, and higher costs for training personnel.

Response: Significant comments were received regarding the cost of systems compliance. In response, the Department retained the assistance of consultants with extensive expertise in health care information technology. We have relied on their work to revise our estimates, as described below. The analysis does not include ''systems compliance'' as a cost item, per se. Rather, in the final analysis we organized estimates around the major policy provisions so the public could more clearly see the costs associated with them. To the extent that the policy might require systems changes (and a number of them do), we have incorporated those costs in the provision's estimate.

Comment: Items explicitly identified by commenters as significantly adding to systems compliance costs include tracking disclosures of protected health information and patient authorizations; restricting access to the data; accommodating minimum disclosure provisions; installing notices and disclaimers; creating de-identified data; tracking uses of protected health information by business partners; tracking amendments and corrections; increased systems capacity; and annual systems maintenance. The commenters noted that some of the aforementioned items are acknowledged in the proposed rule as future costs to covered entities, but several others are singularly ignored.

Response: The Department recognizes the validity of much of this criticism. Unfortunately, other than general criticism, commenters provided no specific data or methodological information which might be used to improve the estimates. Therefore, the Department retained consultants with extensive expertise in these areas to assess the proposed regulation, which helped the Department refine its policies and cost estimates.

In addition, it is important to note that the other HIPAA administrative simplification regulations will require systems changes. As explained generally in the cost analysis for the electronic Transactions rule, it is assumed that providers and vendors will undertake systems changes for these regulations collectively, thereby minimizing the cost of changes.

Inspection and Copying

Comment: Numerous commenters disagreed with the cost estimates in the NPRM for inspection and copying of patient records, believing that they were too low.

Response: The Department has investigated the potential costs through a careful reading of the comments and subsequent factfinding discussions with a variety of providers. We believe the estimates, explained more fully below, represent a reasonable estimate in the aggregate. It is important to note, however, that this analysis is not measuring the cost of all inspection and copying because a considerable amount of this already occurs. The Department is only measuring the incremental increase likely to occur as a result of this regulation.

Comment: One commenter speculates that, even at a minimum charge of $.50/page, (and not including search and retrieval charges), costs could run as high as $450 million annually.

Response: The $0.50 per page in the proposal represent an average of several data sources. Subsequently, an industry commenter, which provided extensive medical records copying, stated that this was a reasonable average cost. Hence, we retained the number for the final estimate.

Comment: One respondent states that, since the proposed rules give patients the right to inspect and copy their medical records regardless of storage medium, HHS must make a distinction in its cost estimates between records stored electronically and those which must be accessed by manual means, since these costs will differ.

Response: The cost estimates made for regulations are not intended to provide such refined gradations; rather, they are intended to show the overall costs for the regulation as a whole and its major components. For inspections and copying (and virtually all other areas for which estimates are made) estimates are based on averages; particular providers may experience greater or lesser costs than the average cost used in this analysis.

Comment: Several commenters noted that the Department did not appear to include the cost of establishing storage systems, retrieval fees and the cost of searching for records, and that these costs, if included, would significantly increase the Department's estimate.

Response: Currently, providers keep and maintain medical records and often provide copies to other providers and patients. Therefore, much of the cost of maintaining records already exists. Indeed, based on public comments, the Department has concluded that there will be relatively few additional copies requested as the result of this regulation (see below). We have measured and attributed to this regulation the incremental cost, which is the standard for conducting this kind of analysis.

Comment: A federal agency expressed concern over the proposal to allow covered entities to charge a fee for copying personal health information based on reasonable costs. The agency requests personal health information from many covered entities and pays a fee that it establishes. Allowing covered entities to establish the fee, the agency fears, may cost them significantly more than the current amounts they pay and as a result, could adversely affect their program.

Response: The proposal and the final rule establish the right to access and copy records only for individuals, not other entities; the ''reasonable fee'' is only applicable to the individual's request. The Department's expectation is that other existing practices regarding fees, if any, for the exchange of records not requested by an individual will not be affected by this rule.

Appending Records (Amendment and Correction)

Comment: The proposed rule estimated the cost of amending and correcting patients' records at $75 per instance and $260 million per year for small entities. At least one commenter stated that such requests will rise significantly upon implementation of the regulations and increase in direct proportion to the number of patients served. Another commenter described the more subtle costs associated with record amendment and correction, which would include a case-by-case clinical determination by providers on whether to grant such requests, forwarding the ensuing record changes to business partners, and issuing written statements to patients on the reasons for denials, including a recourse for complaints.

Response: The comments were considered in revising the proposal, and the decision was made to clarify in the final regulation that providers must only append the record (the policy is explained further in the preamble and the regulation text). The provider is now only required to note in the medical record any comments from the patient; they may, but are not required to, correct any errors. This change in policy significantly reduces the cost from the initial proposal estimate.

Comment: Several commenters criticized the proposed rule's lack of justification for assumptions regarding the percentage of patients who request inspection and copying, who also request amendment and correction. Another commenter pointed out that the cost estimate for amendment and correction is dependent on a base assumption that only 1.5 percent of patients will request inspection of their records. As such, if this estimate were too low by just one percentage point, then the estimates for inspection and copying plus the costs for amendment and correction could rise by 67 percent.

Response: Based on information and data received in the public comments, the estimate for the number of people requesting inspection and copying has been revised. No commenter provided specific information on the number of amended record requests that might result, but the Department subsequently engaged in fact-finding and made appropriate adjustments in its estimates. The revisions are explained further below.

Consent and Authorizations

Comment: One respondent indicated that the development, collection, and data entry of all the authorizations will create a new transaction type for employers, health plans, and providers, and result in duplicated efforts among them. This commenter estimates that the costs of mailing, re-mailing, answering inquiries, making outbound calls and performing data entry in newly created authorization computer systems could result in expenses of close to $2.0 billion nationally. Another commenter indicated that authorization costs will be at least double the notice dissemination costs due to the cost of both outbound and return postage.

Response: Public commenters and subsequent factfinding clearly indicate that most providers with patient contact already obtain authorizations for release of records, so for them there is virtually no new cost. Further, this comment does not reflect the actual regulatory requirement. For example, there is no need to engage in mailing and re-mailing of forms, and we do not foresee any reason why there should be any significant calls involved.

Comment: A commenter criticized the percentage (1%) that we used to calculate the number of health care encounters expected to result in requests to withhold the release of protected information. This respondent postulates that even if one in six patients who encounter the U.S. health care system opt to restrict access to their records, the total expected national cost per year could rise to $900 million.

Response: The final regulation requirements regarding the release of protected health information has been substantially changed, thereby greatly reducing the potential cost burden. A fuller explanation of the cost is provided below in the regulatory impact analysis.

Comment: An additional issue raised by commenters was the added cost of seeking authorizations for health promotion and disease management activities, health care operations that traditionally did not require such action.

Response: In the final regulation, a covered entity can use medical information collected for treatment or operations for its own health promotion and disease management efforts without obtaining additional authorization. Therefore, there is no additional cost incurred.

Business Associates

Comment: A number of commenters were concerned about the cost of monitoring business partners. Specifically, one commenter stated that the provisions of the proposed regulation pertaining to business partners would likely force the discontinuation of outsourcing for some functions, thereby driving up the administrative cost of health care.

Response: The final regulation clarifies the obligations of the business associates in assuring privacy. As explained in the preamble, business associates must take reasonable steps to assure confidentiality of health records they may have, and the covered entity must take appropriate action if they become aware of a violation of the agreement they have with the business associate. This does not represent an unreasonable burden; indeed, the provider is required to take the same kind of precautions and provide the same kind of oversight that they would in many other kinds of contractual relationships to assure they obtain the quality and level of performance that they would expect from a business associate.

Comment: HHS failed to consider enforcement costs associated with monitoring partners and litigation costs arising from covered entities seeking restitution from business partners whose behavior puts the covered entity at risk for noncompliance.

Response: The Department acknowledged in the proposal that it was not estimating the cost of compliance with the business associates provision because of inadequate information. It requested information on this issue, but no specific information was provided in the comments. However, based on revisions in the final policy and subsequent factfinding, the Department has provided an estimate for this requirement, as explained below.

Training

Comment: Many of the commenters believe that the Department used unrealistic assumptions in the development of the estimated cost of the training provisions and they provided their own estimates.

Response: The commenters' estimates varied widely, and could not be used by the Department in revising its analysis because there was inadequate explanation of how the estimates were made.

Comment: Several commenters argued that if even an hour of time of each of the entity's employees is spent on training instead of ''work'' and they are paid the minimum wage, an entity would incur $100 of cost for training no more than 20 employees. The commenters noted that the provision of health care services is a labor-intensive enterprise, and many covered entities have thousands of employees, most of whom make well in excess of minimum

wage. They questioned whether the estimates include time taken from the employee's actual duties (opportunity cost) and the cost of a trainer and materials.

Response: As explained in more detail below, the Department made extensive revisions in its training estimate, including the number of workers in the health care sector, the cost of workers in training based on average industry wages, and training costs (instructors and materials). The revised estimate is a more complete and accurate estimate of the costs likely to be borne as a result of the final regulation.

Comment: One commenter estimated that simply training an employee could have a burdensome impact on his company. He argued, for example, a 10-hour annual requirement takes 0.5% of an employee's time if they work a 2000-hour year, but factoring in sick and vacation leave, the effects of industry turnover could significantly increase the effect.

Response: In the analysis below, the Department has factored in turnover rates, employment growth and greater utilization based on data obtained from broad-based surveys and a public comment.

Comment: Some commenters felt that the regulatory training provisions are overly burdensome. Specific concerns centered around the requirement to train all individuals who may come in contact with protected health information and the requirement to have such individuals sign a new certifying statement at least every three years. Some commenters felt that the content of the training program should be left to the discretion of the covered entity.

Response: Changes and clarifications in the training requirements are made in the final regulation, explained below. For example, the certification requirement has been eliminated. As in the NPRM, the content of the training program is left to the discretion of the covered entity. These changes are expected to lessen the training burden and are reflected in the final cost estimates.

Compliance and Enforcement

Comment: A Member of Congress and a number of privacy and consumer groups expressed their concern with whether the Office for Civil Rights (OCR) in HHS has adequate funding to carry out the major responsibility of enforcing the complaint process established by this rule. The Member stated that ''[d]ue to the limited enforcement ability allowed for in this rule by HIPAA, it is essential that OCR have the capacity to enforce the regulations. Now is the time for The Secretary to begin building the necessary infrastructure to enforce the regulation effectively.''

Response: The Secretary agrees with the commenters and is committed to an effective enforcement program. We will work with Congress to ensure that the Department has the necessary funds to secure voluntary compliance through education and technical assistance, to investigate complaints and conduct compliance reviews, to provide states with exception determinations and to use civil and criminal penalties when necessary.

Economic Effect on Small Entities

Comment: Many commenters stated that the cost estimates on the effect of the proposed regulation on small businesses were understated or incomplete.

Response: The Department conducted a thorough review of potential data sources that would improve the quality of the analysis of the effects on small business. The final regulatory flexibility analysis below is based on the best data available (much of it from the Small Business Administration) and represents a reliable estimate for the effects on small entities in various segments of the health care industry. It is important to note that the estimates are for small business segments in the aggregate; the cost to individual firms will vary, perhaps considerably, based on its particular circumstances.

Comment: The cost of implementing privacy regulations, when added to the cost of other required HIPAA regulations, could increase overhead significantly. As shown in the 1993 Workgroup on Electronic Data Interchange (WEDI) Report, providers will bear the larger share of implementation costs and will save less than payors.

Response: The regulatory flexibility analysis below shows generally the marginal effect of the privacy regulation on small entities. Collectively, the HIPAA administrative standards will save money in the health care system. As important, given the rapid expansion of electronic commerce, it is probable that small entities would need to comply with standards for electronic commerce in order to complete effectively, even if the standards were voluntary. The establishment of uniform standards through regulation help small entities because they will not have to invest in multiple systems, which is what they would confront if the system remained voluntary.

Comment: One respondent believed that the initial and ongoing costs for small provider offices could be as much as 11 times higher than the estimates provided in the proposed rule. Other commenters stated that the estimates for small entities are ''absurdly low''.

Response: Although there were a number of commenters highly critical of the small business analysis, none provided alternative estimates or even provided a rationale for their statements. Many appeared to assume that all costs associated with medical record confidentiality should be estimated. This represents a misunderstanding of the purpose of the analysis: to estimate the incremental effects of this regulation, *i.e.,* the new costs (and savings) that will result from changes required by the regulation. The Department has made substantial changes in the final small entities analysis (below), reflecting policy changes in the final rule and additional information and data collected by the Department since the issuance of the proposal last fall. We believe that these estimates reasonably reflect the costs that various types of small entities will experience in general, though the actual costs of particular providers might vary considerably based on their current practices and technology.

Comment: A respondent expressed the belief that small providers would bear a disproportionate share of the regulation's administrative burden because of the likelihood of larger companies incurring fewer marginal costs due to greater in-house resources to aid in the legal and technical analysis of the proposed rule.

Response: As explained below, the Department does not agree with the assertion that small entities will be disproportionately affected. Based on discussions with a number of groups, the Department expects many professional and trade associations to provide their members with analysis of the regulation, including model policies, statements and basic training materials. This will minimize the cost for most small entities. Providers that use protected health information for voluntary practices, such as marketing or research, are more likely to need specific legal and technical assistance, but these are likely to be larger providers.

Comment: Several commenters took issue with the ''top-down'' approach that we used to estimate costs for small businesses, believing that this methodology provided only a single point estimate, gave no indication of the variation around the estimate, and was subject to numerous methodological errors since the entities to which the numerator pertained may not have been

the same as the denominator. These respondents further recommended that we prepare a ''bottom-up'' analysis using case studies and/or a survey of providers to refine the estimates.

Response: The purpose of the regulatory flexibility analysis is to provide a better insight into the relative burden of small businesses compared to larger firms in complying with a regulation. There may be considerable variance around average costs within particular industry sectors, even among small businesses within them. The estimates are based on the best data available, including information from the Small Business Administration, the Census Bureau, and public comments.

Comment: A commenter stated that the proposal's cost estimate does not account for additional administrative costs imposed on physicians, such as requirements to rewrite contracts with business partners.

Response: Such costs are included in the analysis below.

Comment: Numerous public comments were directed specifically at the systems compliance cost estimates for small businesses. One respondent maintained that the initial upgrade cost alone would range from $50 thousand to more than $1 million per covered entity.

Response: The cost estimates for systems compliance varied enormously; unfortunately, none of the commenters provided documentation of how they made their estimates, preventing us from comparing their data and assumptions to the Department's. Because of concern about the costs in this area, however, the Department retained an outside consultant to provide greater expertise and analysis. The product of this effort has been incorporated in the analysis below.

Comment: One commenter stated that just the development and documentation of new health information policies and procedures (which would require an analysis of the federal regulations and state law privacy provisions), would cost far more than the $396 cited in the Notice of Proposed Rulemaking as the average start-up cost for small businesses.

Response: As explained below in the cost analysis, the Department anticipates that most of the policies and procedures that will be required under the final rule will be largely standardized, particularly for small businesses. Thus, much of the work and cost can be done by trade associations and professional groups, thereby minimizing the costs and allowing it to be spread over a large membership base.

Comment: A number of comments criticized the initial estimates for notices, inspection and copying, amendments and correction, and training as they relate to small businesses.

Response: The Department has made substantial revisions in its estimates for all of these areas which is explained below in the regulatory flexibility analysis.

Comment: One commenter noted that there appeared to be a discrepancy in the number of small entities cited. There is no explanation for the difference and no explanation for difference between ''establishments'' and ''entities.''

Response: There are discrepancies among the data bases on the number of ''establishments'' and ''entities'' or ''firms''. The problem arises because most surveys count (or survey) establishments, which are physical sites. A single firm or entity may have many establishments. Moreover, although an establishment may have only a few employees, the firm may have a large number of workers (the total of all its various establishments) and therefore not be a small entity.

As discussed below, there is some discrepancy between the aggregate numbers we use for the regulatory impact analysis (RIA) and the regulatory flexibility analysis (RFA). We concluded that for purposes of the RFA, which is intended to measure the effects on small entities, we would use Small Business Administration data, which defines entities based on revenues rather than physical establishments to count the number of small entities in various SIC. This provides a more accurate estimate of small entities affected. For the RIA, which is measuring total effects, we believe the establishment based surveys provide a more reliable count.

Comment: Because small businesses must notify patients of their privacy policies on patients' first visit after the effective date of the regulation, several commenters argued that staff would have to search records either manually or by computer on a daily basis to determine if patients had been seen since the regulation was implemented.

Response: Under the final regulation, all covered entities will have to provide patients copies of their privacy policy at the first visit after the effective date of the regulation. The Department does not view this as burdensome. We expect that providers will simply place a note or marker at the beginning of a file (electronic or paper) when a patient is given the notice. This is neither time-consuming nor expensive, and it will not require constant searches of records.

Comment: A commenter stated that the definitions of small business, small entity, and a small health plan are inconsistent because the NPRM includes firms with annual receipts of $5 million or less and non-profits.

Response: The Small Business Administration, whose definitions we use for this analysis, includes firms with $5 million or less in receipts and all non-profits as ''small businesses.'' We recognize that some health plans, though very large in terms of receipts (and insured lives), nonetheless would be considered ''small businesses'' under this definition because they are non-profits. In the final regulatory flexibility analysis, we generally have maintained the Small Business Administration definitions because it is the accepted standard for these analyses. However, we have added several categories, such as IRBs and employer sponsored group health plans, which are not small entities, per se, but will be effected by the final rule and we were able to identify costs imposed by the regulation on them.

Comment: The same commenter wanted clarification that all non-profit organizations are small entities and that the extended effective date for compliance applies to them.

Response: For purposes of the regulatory flexibility analysis, the Department is utilizing the Small Business Administration guidelines. However, under HIPAA the Secretary may extend the effective compliance date from 24 months to 36 months for ''small health plans''. The Secretary is given the explicit discretion of defining the term for purposes of compliance with the regulation. For compliance purposes, the Secretary has decided to define ''small health plans'' as those with receipts of $5 million or less, regardless of their tax status. As noted above, some non-profit plans are large in terms of revenues (*i.e.,* their revenues exceed $5 million annually). The Department determined that such plans do not need extra time for compliance.

Comment: Several commenters requested that ''small providers'' [undefined] be permitted to take 36 months to come into compliance with the final regulation, just as small health plans will be permitted to do so.

Response: Congress specified small health plans, but not small providers, as needing extra time to comply. The majority of providers affected by the regulation are ''small'', based on the SBA definitions; in other words, granting the delay would be tantamount to make the effective date three years rather than two. In making policy decisions for the final regulation, extensive consideration was given to minimizing the cost and administrative burden associated with implementing

the rule. The Department believes that the requirements of the final rule will not be difficult to fulfill, and therefore, it has maintained the two year effective date.

External Studies

Comment: One commenter submitted a detailed analysis of privacy legislation that was pending and concluded that they might cost over $40 billion.

Response: The study did not analyze the policies in the proposal, and therefore, the estimates do not reflect the costs that would have been imposed by the proposed regulation. In fact, the analysis was prepared before the Administration's proposed privacy regulation was even published. As a result, the analysis is of limited relevance to the regulation actually proposed.

The following are examples of assumptions and costs in the analysis that do not match privacy policies or requirements stated in the proposed rule.

1. *Authorizations:* The study assumed rules requiring new authorizations from current subscribers to use their data for treatment, payment of claims, or other health plan operations. The proposed rule would have prohibited providers or plans from obtaining patient authorization to use data for treatment, payment or health care operations, and the final rule makes obtaining consent for these purposes voluntary for all health plans and for providers that do not have direct treatment relationships with individuals.

2. *Disclosure History:* The study assumes that providers, health plans, and clearinghouses would have to track all disclosures of health information. Under the NPRM and the final rule, plans, providers and clearinghouses are only required to account for disclosures that are not for treatment, payment, and health care operations, a small minority of all disclosures.

3. *Inspection, Copying, and Amendment:* The study assumed requirements to allow patients and their subscribers to inspect, copy, and amend all information that includes their name, social security number or other identifying feature (*e.g.* customer service calls, internal memorandum, claim runs). However, the study assumed broader access than provided in the rule, which requires access only to information in records used to make decisions about individuals, not all records with identifiable information.

4. *Infrastructure development:* The study attributed significant costs to infrastructure implementation of (computer systems, training, and other compliance costs). As explained below, the compliance requirements are much less extensive than assumed in this study. For example, many providers and plans will not be required to modify their privacy systems but will only be required to document their practices and notify patients of these practices, and others will be able to purchase low-cost, off-the-shelf software that will facilitate the new requirements. The final regulation will not require massive capital expenditures; we assumed, based on our consultants' work, that providers will rely on low-cost incremental adjustments initially, and as their technology becomes outdated, they will replace it with new systems that incorporate the HIPAA standard requirements.

Although many of the policy assumptions in the study are fundamentally different than those in the proposed or final regulation, the study did provide some assistance to the Department in preparing its final analysis. The Department compared data, methodologies and model assumptions, which helped us think more critically about our own analysis and enhanced the quality of our final work.

Comment: One commenter submitted a detailed analysis of the NPRM Regulatory Impact Analysis and concluded that it might cost over $64 billion over 5 years. This analysis provided an interesting framework for analyzing the provision for the rule. More precisely, the analysis generally attempted to identify the number of entities would be required to comply with each of the significant provision of the proposed rule, then estimated the numbers of hours required to comply per entity, and finally, estimated an hourly wage.

Response: HHS adopted this general structure for the final RIA because it provided a better framework for analysis than what the Department had done in the NPRM. However, HHS did not agree with many of the specific assumptions used by in this analysis, for several reasons. First, in some instances the assumptions were no longer relevant because the requirements of the NPRM were altered in the final rule. For other assumptions, HHS found more appropriate data sources for the number of covered entities, wages rates and trend rates or other factors affecting costs. In addition, HHS believes that in a few instances, this analysis over-estimated what is required of covered entities to comply. Based on public comments and its own factfinding, the Department believes many of its assumptions used in the final analysis more accurately reflect what is likely to be the real cost of the regulation.

IV. Final Regulatory Impact Analysis

5 U.S.C. 804(2) (as added by section 251 of Pub. L. 104–21), specifies that a ''major rule'' is any rule that the Office of Management and Budget finds is likely to result in:

- An annual effect on the economy of $100 million or more;
- A major increase in costs or prices for consumers, individual industries, federal, state, or local government agencies, or geographic regions; or
- Significant adverse effects in competition, employment, investment productivity, innovation, or on the ability of United States based enterprises to compete with foreign-based enterprises in domestic and export markets. The impact of this final rule will be over $1 billion in the first year of implementation. Therefore, this rule is a major rule as defined in 5 U.S.C. 804(2).

Executive Order 12866 directs agencies to assess all costs and benefits of available regulatory alternatives and, when regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects; distributive impacts; and equity). According to Executive Order 12866, a regulatory action is ''significant'' if it meets any one of a number of specified conditions, including having an annual effect on the economy of $100 million or more adversely affecting in a material way a sector of the economy, competition, or jobs, or if it raises novel legal or policy issues. The purpose of the regulatory impact analysis is to assist decision-makers in understanding the potential ramifications of a regulation as it is being developed. The analysis is also intended to assist the public in understanding the general economic ramifications of a regulation, both in the aggregate as well as the major policy areas of a regulation and how they are likely to affect the major industries or sectors of the economy covered by it.

In accordance with the Small Business Regulatory Enforcement and Fairness Act (Pub. L. 104–121), the Administrator of the Office of Information and Regulatory Affairs of the Office of Management and Budget (OMB) has determined that this rule is a major rule for the purpose of congressional review.

The proposal for the privacy regulation included a preliminary regulatory impact analysis (RIA) which estimated the cost of the rule at $3.8 billion over five years. The preliminary

analysis also noted that a number of significant areas were not included in the estimate due to inadequate information. The proposal solicited public comment on these and all other aspects of the analysis. In this preamble, the Department has summarized the public comments pertinent to the cost analysis and its response to them. However, because of the extensive policy changes incorporated in the final regulation, additional data collected from the public comments and the Department's fact-finding, and changes in the methodology underlying the estimates, the Department is setting forth in this section a more complete explanation of its revised estimates and how they were obtained. This will facilitate a better understanding by the public of how the estimates were developed and provide more insight into how the Department believes the regulation will ultimately affect the health care sector.

The impact analysis measures the effect of the regulation on current practices. In the case of privacy, as discussed in the preamble, there already exists considerable, though quite varied, efforts to protect the confidentiality of medical information. The RIA is measuring the change in these current practices and the cost of new and additional responsibilities that are required to conform to the new regulation.

To achieve a reasonable level of privacy protection, the Department defined three objectives for the final rule: (1) To establish national baseline standards, implementation specifications, and requirements for health information privacy protection, (2) to protect the privacy of individually identifiable health information maintained or transmitted by covered entities, and (3) to protect the privacy of all individually identifiable health information within covered entities, regardless of its form.

Establishing minimum standards, implementation specifications, and requirements for health information privacy protection creates a level baseline of privacy protection for patients across states. The Health Privacy Project's report, *The State of Health Privacy: An Uneven Terrain* [33] makes it clear that under the current system of state laws, privacy protection is extremely variable. The Department's statutory authority under HIPAA which allows the privacy regulation to preempt any state law if such law is contrary to and not more stringent than privacy protection pursuant to this regulation. This sets a floor, but permits a state to create laws that are more protective of privacy. We discuss preemption in greater detail in other parts of the preamble.

The second objective is to establish a uniform base of privacy protection for individually identifiable health information maintained or transmitted by covered entities. HIPAA restricts the type of entities covered by the rule to three broad categories: health care providers that transmit health information in HIPAA standard transactions, health plans, and health care clearinghouses. However, there are similar public and private entities that are not within the Department's authority to regulate under HIPAA. For example, life insurance companies are not covered by this rule but may have access to a large amount of individually identifiable health information.

The third objective is to protect the privacy of all individually identifiable health information held by covered entities, including their business associates. Health information is currently stored and transmitted in multiple forms, including electronic, paper, and oral forms. To provide consistent protection to information, and to avoid requiring covered entities from distinguishing between health information that has been transmitted or maintained electronically and that which has not, this rule covers all individually identifiable health information in any form maintained or transmitted by a covered entity.

For purposes of this cost analysis, the Department has assumed all health care providers will be affected by the rule. This results in an overestimation of costs because there are providers that do not engage in any HIPAA standard transactions, and therefore, are not affected. The Department could not obtain any reliable data on the number of such providers, but the available data suggest that there are very few such entities, and given the expected increase in all forms of electronic health care in the coming decade, the number of paper-only providers is likely to decrease.

A. Relationship of This Analysis to Analyses in Other HIPAA Regulations

Congress has recognized that privacy standards, implementation specifications and requirements must accompany the electronic data interchange standards, implementation specifications and requirements because the increased ease of transmitting and sharing individually identifiable health information will result in an increase in concern regarding privacy and confidentiality of such information. The bulk of the first Administrative Simplification section that was debated on the floor of the Senate in 1994 (as part of the Health Security Act) was made up of privacy provisions. The requirement for the issuance of concomitant privacy measures remained a part of the HIPAA bill passed by the House of Representatives in 1996, but the requirement for privacy measures was removed in conference. Instead, Congress added section 264 to Title II of HIPAA, which directs the Secretary to develop and submit to Congress recommendations addressing at least the following:

(1) The rights that an individual who is a subject of individually identifiable health information should have.

(2) The procedures that should be established for the exercise of such rights.

(3) The uses and disclosures of such information that should be authorized or required. The Secretary's Recommendations were submitted to Congress on September 11, 1997, and are summarized below. Section 264(c)(1) of HIPAA provides that: If legislation governing standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a) of the Social Security Act (as added by section 262) is not enacted by (August 21, 1999), the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than (February 21, 2000). Such regulations shall address at least the subjects described in subsection (regarding recommendations).

Because the Congress did not enact legislation governing standards with respect to the privacy of individually identifiable health information prior to August 21, 1999, the Department has, in accordance with this statutory mandate, developed final rules setting forth standards to protect the privacy of such information.

Title II of the Health Insurance Portability and Accountability Act (HIPAA) also provides a statutory framework for the promulgation of other administrative simplification regulations. On August 17, 2000, the Transactions Rule was published. Proposals for health care provider identifier (May 1998), employer identifier (June 1998), and security and electronic signature standards (August 1998) have also been published. These

[33] Janlori Goldman, Institute for Health Care Research and Policy, Georgetown University: <http://www.healthprivacy.org/resources>.

regulations are expected to be made final in the foreseeable future.

HIPAA states that, ''any standard adopted under this part shall be consistent with the objective of reducing the administrative costs of providing and paying for health care.'' (Section 1172 (b)). This provision refers to the administrative simplification regulations in their totality, including this rule regarding privacy standards. The savings and costs generated by the various standards should result in a net savings to the health care system. The Transactions Rule shows a net savings of $29.9 billion over ten years (2002–2011), or a net present value savings of $19 billion. This estimate does not include the growth in ''e-health'' and ''e-commerce'' that may be spurred by the adoption of uniform codes and standards.

This final Privacy Rule is estimated to produce net costs of $18.0 billion, with net present value costs of $11.8 billion (2003 dollars) over ten years (2003–2012). This estimate is based on some costs already having been incurred due to the requirements of the Transactions Rule, which included an estimate of a net savings to the health care system of $29.9 billion over ten years (2002 dollars) and a net present value of $19.1 billion. The Department expects that the savings and costs generated by all administrative simplification standards should result in a net savings to the health care system.

B. Summary of Costs and Benefits

Measuring both the economic costs and benefits of health information privacy is difficult. Traditionally, privacy has been addressed by state laws, contracts, and professional practices and guidelines. Moreover, these practices have been evolving as computers have dramatically increased the potential use of medical data; the scope and form of health information is likely to be very different ten years from now than it is today. This final regulation is both altering current health information privacy practice and shaping its evolution as electronic uses expand.

To estimate costs, the Department used information from published studies, trade groups and associations, public comments to the proposed regulation, and fact-finding by staff. The analysis focused on the major policy areas in the regulation that would result in significant costs. Given the vast array of institutions affected by this regulation and the considerable variation in practices, the Department sought to identify the ''typical'' current practice for each of the major policy areas and estimate the cost of change resulting from the regulation. Because of the paucity of data and incomplete information on current practices, the Department has consistently made conservative assumptions (that is, given uncertainty, we have made assumptions that, if incorrect, are more likely to overstate rather than understate the true cost).

Benefits are difficult to measure because people conceive of privacy primarily as a right, not as a commodity. Furthermore, a wide gap appears to exist between what people perceive to be the level of privacy afforded health information about them and what actually occurs with the use of such information today. Arguably, the ''cost'' of the privacy regulation is the amount necessary to bring health information privacy to these perceived levels.

The benefits of enhanced privacy protections for individually identifiable health information are significant, even though they are hard to quantify. The Department solicited comments on this issue, but no commenters offered a better alternative. Therefore, the Department is essentially reiterating the analysis it offered in the proposed Privacy Rule. The illustrative examples set forth below, using existing data on mental health, cancer screening, and HIV/AIDS patients, suggest the level of economic and health benefits that might accrue to individuals and society. Moreover, the benefits of improved privacy protection are likely to increase in the future as patients gain trust in health care practitioners' ability to maintain the confidentiality of their health information.

The estimated cost of compliance with the final rule is $17.6 billion over the ten year period, 2003–2012.[34] This includes the cost of all the major requirements for the rule, including costs to federal, state and local governments. The net present value of the final rule, applying a 11.2 percent discount rate[35], is $11.8 billion.[36]

The first year estimate is $3.2 billion (this includes expenditures that may be incurred before the effective date in 2003). This represents about 0.23 percent of projected national health expenditures for 2003.[37] By 2008, seven years after the rule's effective date, the rule is estimated to cost 0.07 percent of projected national health expenditures.

The largest cost items are the requirement to have a privacy official, $5.9 billion over ten years, and the requirement that disclosures of protected health information only involve the minimum amount necessary, $5.8 billion over ten years (see Table 1). These costs reflect the change that affected organizations will have to undertake to implement and maintain compliance with the requirements of the rule and achieve enhanced privacy of protected health information.

[34] The proposed privacy rule provided an estimate for a five-year period. However, the Transactions Rule provided a cost estimate for a ten year period. The decision was made to provide the final privacy estimates in a ten year period so that it would be possible to compare the costs and benefits of the two regulations.

[35] This based on a seven percent real discount rate, explained in OMB Circular A–94, and a projected 4.2 percent inflation rate projected over the ten-year period covered by this analysis.

[36] The regulatory impact analysis in the Transactions Rule showed a net savings of $29.9 billion (net present value of $19.1 billion in 2002 dollars). The cost estimates included all electronic systems changes that would be necessitated by the HIPAA administrative standards (*e.g.,* security, safeguards, and electronic signatures; eligibility for a health plan; and remittance advice and payment claim status), except privacy. At the time the Transactions Rule was developed, the industry provided estimates for the systems changes in the aggregate. The industry argued that affected parties would seek to make all electronic changes in one effort because that approach would be the most cost-efficient. The Department agreed, and therefore, it ''bundled'' all the system change cost in the Transactions Rule estimate. Privacy was not included because at the time the Department had not made a decision to develop a privacy rule. As the Department develops other HIPAA administrative simplification standards, there may be additional costs and savings due to the non-electronic components of those regulations, and they will be identified in regulatory impact analyses that accompany those regulations. The Department anticipates that such costs and savings will be relatively small compared to the privacy and Transactions rules. The Department anticipates that the net economic impact of the rules will be a net savings to the health care system.

[37] Health spending projections from *National Health Expenditure Projections 1998–2008* (January 2000), Health Care Financing Administration, Office of the Actuary, <*http://hcfa.hhs.gov/stats/nhe-proj/*>.

from national surveys while preserving confidentiality and which have been dealing with these issues for decades. The problems and solutions being used by these agencies are laid out in detail in the Statistical Policy Working Paper 22 cited earlier.

To protect the privacy of individuals providing information to the Bureau of Census, the Bureau has determined that a geographical region must contain at least 100,000 people.[20] This standard has been used by the Bureau of the Census for many years and is supported by simulation studies using Census data.[21] These studies showed that after a certain point, increasing the size of a geographic area does not significantly decrease the percentage of unique records (i.e., those that could be identified if sampled), but that the point of diminishing returns is dependent on the number and type of demographic variables on which matching might occur. For a small number of demographic variables (6), this point was quite low (about 20,000 population), but it rose quickly to about 50,000 for 10 variables and to about 80,000 for 15 variables. The Bureau of the Census releases sets of data to the public that it considers safe from re-identification because it limits geographical areas to those containing at least 100,000 people and limits the number and detail of the demographic variables in the data. At the point of approximately 100,000 population, 7.3% of records were unique (and therefore potentially identifiable) on 6 demographic variables from the 1990 Census Short Form: Age in years (90 categories), race (up to 180 categories), sex (2 categories), relationship to householder (14 categories), Hispanic (2 categories), and tenure (owner vs. renter in 5 categories). Using 6 variables derived from the Long Form data, age (10 categories), race (6 categories), sex (2 categories), marital status (5 categories), occupation (54 categories), and personal income (10 categories), raised the percentage to 9.8%.

We also examined the results of an NCHS simulation study using national survey data[22] to see if some scientific support could be found for a compromise. The study took random samples from populations of different sizes and then compared the samples to the whole population to see how many records were identifiable, that is, matched uniquely to a unique person in the whole population on the basis of 9 demographic variables: Age (85 categories), race (4 categories), gender (2 categories), ethnicity (2 categories), marital status (3 categories), income (3 categories), employment status (2 categories), working class (4 categories), and occupation (42 categories). Even when some of the variables are aggregated or coded, from the perspective of a large statistical agency desiring to release data to the public, the study concluded that a population size of 500,000 was not sufficient to provide a reasonable guarantee that certain individuals could not be identified. About 2.5 % of the sample from the population of 500,000 was uniquely identifiable, regardless of sample size. This percentage rose as the size of the population decreased, to about 14% for a population of 100,000 and to about 25% for a population of 25,000. Eliminating the occupation variable (which is less likely to be found in health data) reduced this percentage significantly to about 0.4 %, 3%, and 10% respectively. These percentages of unique records (and thus the potentials for re-identification) are highly dependent on the number of variables (which must also be available in other databases which are identified to be considered in a disclosure risk analysis), the categorical breakdowns of those variables, and the level of geographic detail included.

With respect to how we might clarify the requirement to achieve a ''low probability'' that information could be identified, the Statistical Policy Working Paper 22 referenced above discusses the attempts of several researchers to define mathematical measures of disclosure risk only to conclude that ''more research into defining a computable measure of risk is necessary.'' When we considered whether we could specify a maximum level of risk of disclosure with some precision (such as a probability or risk of identification of <0.01), we concluded that it is premature to assign mathematical precision to the ''art'' of de-identification.

After evaluating current practices and recognizing the expressed need for some geographic indicators in otherwise de-identified databases, we concluded that permitting geographic identifiers that define populations of greater than 20,000 individuals is an appropriate standard that balances privacy interests against desirable uses of de-identified data. In making this determination, we focused on the studies by the Bureau of Census cited above which seemed to indicate that a population size of 20,000 was an appropriate cut off if there were relatively few (6) demographic variables in the database. Our belief is that, after removing the required identifiers to meet the safe harbor standards, the number of demographic variables retained in the databases will be relatively small, so that it is appropriate to accept a relatively low number as a minimum geographic size.

In applying this provision, covered entities must replace the (currently 18) forbidden 3-digit zip codes with zeros and thus treat them as a single geographic area (with >20,000 population). The list of the forbidden 3-digit zip codes will be maintained as part of the updated Secretarial guidance referred to above. Currently, they are: 022, 036, 059, 102, 203, 555, 556, 692, 821, 823, 830, 831, 878, 879, 884, 893, 987, and 994. This will result in an average 3-digit zip code area population of 287,858 which should result in an average of about 4% unique records using the 6 variables described above from the Census Short Form. Although this level of unique records will be much higher in the smaller geographic areas, the actual risk of identification will be much lower because of the limited availability of comparable data in publically available, identified databases, and will be further reduced by the low probability that someone will expend the resources to try to identify records when the chance of success is so small and uncertain. We think this compromise will meet the current need for an easy method to identify geographic area while providing adequate protection from re-identification. If a greater level of geographical detail is required for a particular use, the information will have to be obtained through another permitted mechanism or be subjected to a specific de-identification determination as described above. We will monitor the availability of identified public data and the concomitant re-identification risks, both theoretical and actual, and adjust this safe harbor in the future as necessary.

As we stated above, we understand that many commenters would prefer a looser standard for determining when information is de-identified, both generally and with respect to the standards for identifying geographic

[20] Statistical Policy Working Paper 22—Report on Statistical Disclosure Limitation Methodology (*http://www.fcsm.gov/working-papers/wp22.html*) (prepared by the Subcommittee on Disclosure Limitation Methodology, Federal Committee on Statistical Methodology, Office of Management and Budget).

[21] The Geographic Component of Disclosure Risk for Microdata. Brian Greenberg and Laura Voshell. Bureau of the Census Statistical Research Division Report: Census/SRD/RR–90–13, October, 1990.

[22] A Simulation Study of the Identifiability of Survey Respondents when their Community of Residence is Known. John Horm, Natonal Center for Health Statistics, 2000.

area. However, because public databases (such as voter records or driver's license records) that include demographic information about a geographically defined population are available, a surprisingly large percentage of records of health information that contain similar demographic information can be identified. Although the number of these databases seems to be increasing, the number of demographic variables within them still appears to be fairly limited. The number of cases of privacy violation from health records which have been identified in this way is small to date. However, the risk of identification increases with decreasing population size, with increasing amounts of demographic information (both in level of detail and number of variables), and with the uniqueness of the combination of such information in the population. That is, an 18-year-old single white male student is not at risk of identification in a database from a large city such as New York. However, if the database were about a small town where most of the inhabitants were older, retired people of a specific minority race or ethnic group, that same person might be unique in that community and easily identified. We believe that the policy that we have articulated reaches the appropriate balance between reasonably protecting privacy and providing a sufficient level of information to make de-identified databases useful.

Comments: Some comments noted that identifiers that accompany photographic images are often needed to interpret the image and that it would be difficult to use the image alone to identify the individual.

Response: We agree that our proposed requirement to remove all photographic images was more than necessary. Many photographs of lesions, for example, which cannot usually be used alone to identify an individual, are included in health records. In this final rule, the only absolute requirement is the removal of full-face photographs, and we depend on the ''catch-all'' of ''any other unique * * * characteristic * * * '' to pick up the unusual case where another type of photographic image might be used to identify an individual.

Comments: A number of commenters felt that the proposed bar for removal had been set too high; that the removal of these 19 identifiers created a difficult standard, since some identifiers may be buried in lengthy text fields.

Response: We understand that some of the identifiers on our list for removal may be buried in text fields, but we see no alternative that protects privacy. In addition, we believe that such unstructured text fields have little or no value in a de-identified information set and would be removed in any case. With time, we expect that such identifiers will be kept out of places where they are hard to locate and expunge.

Comments: Some commenters asserted that this requirement creates a disincentive for covered entities to de-identify data and would compromise the Secretary's desire to see de-identified data used for a multitude of purposes. Others stated that the ''no reason to believe'' test creates an unreasonable burden on covered entities, and would actually chill the release of de-identified information, and set an impossible standard.

Response: We recognize that the proposed standards might have imposed a burden that could have prevented the widespread use of de-identified information. We believe that our modifications to the final rule discussed above will make the process less burdensome and remove some of the disincentive. However, we could not loosen the standards as far as many commenters wanted without seriously jeopardizing the privacy of the subjects of the information. As discussed above, we modify the ''no reason to know'' standard that was part of the safe harbor provision and replace it in the final rule with an ''actual knowledge'' standard. We believe that this change provides additional certainty to covered entities using the safe harbor and should eliminate any chilling effect.

Comments: Although most commenters wanted to see data elements taken off the list, there were a small number of commenters that wanted to see data items added to the list. They believed that it is also necessary to remove clinical trial record numbers, device model serial numbers, and all proper nouns from the records.

Response: In response to these requests, we have slightly revised the list of identifiers that must be removed under the safe harbor provision. Clinical trial record numbers are included in the general category of ''any other unique identifying number, characteristic, or code.'' These record numbers cannot be included with de-identified information because, although the availability of clinical trial numbers may be limited, they are used for other purposes besides de-identification/re-identification, such as identifying clinical trial records, and may be disclosed under certain circumstances. Thus, they do not meet the criteria in the rule for use as a unique record identifier for de-identified records. Device model serial numbers are included in ''any device identifier or serial number'' and must be removed. We considered the request to remove all proper nouns to be very burdensome to implement for very little increase in privacy and likely to be arbitrary in operation, and so it is not included in the final rule.

Re-Identification

Comments: One commenter wanted to know if the rule requires that covered entities retain the ability to re-identify de-identified information.

Response: The rule does not require covered entities to retain the ability to re-identify de-identified information, but it does allow them to retain this ability.

Comments: A few commenters asked us to prohibit anyone from re-identifying de-identified health information.

Response: We do not have the authority to regulate persons other than covered entities, so we cannot affect attempts by entities outside of this rule to re-identify information. Under the rule, we permit the covered entity that created the de-identified information to re-identify it. However, we include a requirement that, when a unique record identifier is included in the de-identified information, such identifier must not be such that someone other than the covered entity could use it to identify the individual (such as when a derivative of the individual's name is used as the unique record identifier).

Section 164.514(d)—Minimum Necessary

Comment: A large number of commenters objected to the application of the proposed ''minimum necessary'' standard for uses and disclosures of protected health information to uses and disclosures for treatment purposes. Some suggested that the final regulation should establish a good faith exception or safe harbor for disclosures made for treatment.

The overwhelming majority of commenters, generally from the medical community, argued that application of the proposed standard would be contrary to sound medical practice, increase medical errors, and lead to an increase in liability. Some likened the standard to a ''gag clause'' in that it limited the exchange of information critical for quality patient care. They found the standard unworkable in daily treatment situations. They argued that this standard would be potentially dangerous in that it could cause practitioners to withhold information that could be essential for later care. Commenters asserted that caregivers need to be able to give and receive a

complete picture of the patient's health to make a diagnosis and develop a treatment plan.

Other commenters noted that the complexity of medicine is such that it is unreasonable to think that anyone will know the exact parameters of the information another caregiver will need for proper diagnosis and treatment or that a plan will need to support quality assurance and improvement activities. They therefore suggested that the minimum necessary standard be applied instead as an administrative requirement.

Providers also emphasized that they already have an ethical duty to limit the sharing of unnecessary medical information, and most already have well-developed guidelines and practice standards in place. Concerns were also voiced that attempts to provide the minimum necessary information in the treatment setting would lead to multiple editions of a record or creation of summaries that turn out to omit crucial information resulting in confusion and error.

Response: In response to these concerns, we substantially revise the minimum necessary requirements. As suggested by certain commenters, we provide, in § 164.502(b), that disclosures of protected health information to or requests by health care providers for treatment are not subject to the minimum necessary standard. We also modify the requirements for uses of protected health information. This final rule requires covered entities to make determinations of minimum necessary use, including use for treatment purposes, based on the role of the person or class of workforce members rather than at the level of specific uses. A covered entity must establish policies and procedures that identify the types of persons who are to have access to designated categories of information and the conditions, if any, of that access. We establish no requirements specific to a particular use of information. Covered entities are responsible for establishing and documenting these policies and procedures. This approach is consistent with the argument of many commenters that guidelines and practice standards are appropriate means for protecting the privacy of patient information.

Comment: Some commenters argued that the standard should be retained in the treatment setting for uses and disclosures pertaining to mental health information. Some of these commenters asserted that other providers do not need to know the mental status of a patient for treatment purposes.

Response: We agree that the standard should be retained for uses of mental health information in the treatment setting. However, we believe that the arguments for excepting disclosures of protected health information for treatment purposes from application of the minimum necessary standard are also persuasive with respect to mental health information. An individual's mental health can interact with proper treatment for other conditions in many ways. Psychoactive medications may have harmful interactions with drugs routinely prescribed for other purposes; an individual's mental health history may help another health care provider understand the individual's ability to abide by a complicated treatment regimen. For these reasons, it is also not reasonable to presume that, in every case, a health care provider will not need to know an individual's mental health status to provide appropriate treatment.

Providers' comments noted existing ethical duties to limit the sharing of unnecessary medical information, and well-developed guidelines and practice standards for this purpose. Under this rule, providers may use these tools to guide their discretion in disclosing health information for treatment.

Comment: Several commenters urged that covered entities should be required to conspicuously label records to show that they are not complete. They argued that absent such labeling, patient care could be compromised.

Response: We believe that the final policy to except disclosures of protected health information for treatment purposes from application of the minimum necessary standard addresses these commenters' concerns.

Comment: Some commenters argued that the audit exception to the minimum necessary requirements needs to be clarified or expanded, because ''audit'' and ''payment'' are essentially the same thing.

Response: We eliminate this exception. The proposed exclusion of disclosures to health plans for audit purposes is replaced with a general requirement that covered entities must limit requests to other covered entities for individually identifiable health information to what is reasonably necessary for the purpose intended.

Comment: Many commenters argued that the proposed standard was unworkable as applied to ''uses'' by a covered entity's employees, because the proposal appeared not to allow providers to create general policy as to the types of records that particular employees may have access to but instead required that each decision be made ''individually,'' which providers interpret as ''case-by-case.'' Commenters argued that the standard with regard to ''uses'' would be impossible to implement and prohibitively expensive, requiring both medical and legal input to each disclosure decision.

Some commenters recommended deletion of the minimum necessary standard with regard to ''uses.'' Other commenters specifically recommended deletion of the requirement that the standard be applied on an individual, case-by-case basis. Rather, they suggested that the covered entity be allowed to establish general policies to meet the requirement. Another commenter similarly urged that the standard not apply to internal disclosures or for internal health care operations such as quality improvement/assurance activities. The commenter recommended that medical groups be allowed to develop their own standards to ensure that these activities are carried out in a manner that best helps the group and its patients.

Other commenters expressed confusion and requested clarification as to how the standard as proposed would actually work in day-to-day operations within an entity.

Response: Commenters' arguments regarding the workability of this standard as proposed were persuasive, and we therefore make significant modification to address these comments and improve the workability of the standard. For all uses and many disclosures, we require covered entities to include in their policies and procedures (see § 164.530), which may be standard protocols, for ''minimum necessary'' uses and disclosures. We require implementation of such policies in lieu of making the ''minimum necessary'' determination for each separate use and disclosure.

For uses, covered entities must implement policies and procedures that restrict access to and use of protected health information based on the specific professional roles of members of the covered entity's workforce. The policies and procedures must identify the persons or classes of persons in the entity's workforce who need access to protected health information to carry out their duties and the category or categories of protected health information to which such persons or classes need access. These role-based access rules must also identify the conditions, as appropriate, that would apply to such access. For example, an institutional health care provider could allow physicians access to all records under the condition that the viewing of medical records of patients not under their care is recorded and reviewed. Other health professionals' access could

be limited to time periods when they are on duty. Information available to staff who are responsible for scheduling surgical procedures could be limited to certain data. In many instances, use of order forms or selective copying of relevant portions of a record may be appropriate policies to meet this requirement.

Routine disclosures also are not subject to individual review; instead, covered entities must implement policies and procedures (which may be standard protocols) to limit the protected health information in routine disclosures to the minimum information reasonably necessary to achieve the purpose of that type of disclosure. For non-routine disclosures, a covered entity must develop reasonable criteria to limit the protected health information disclosed to the minimum necessary to accomplish the purpose for which disclosure is sought, and to implement procedures for review of disclosures on an individual basis.

We modify the proposed standard to require the covered entity to make ''reasonable efforts'' to meet the minimum necessary standard (not ''all'reasonable efforts, as proposed). What is reasonable will vary with the circumstances. When it is practical to use order forms or selective copying of relevant portions of the record, the covered entity is required to do so. Similarly, this flexibility in the standard takes into account the ability of the covered entity to configure its record system to allow selective access to only certain fields, and the practicality of organizing systems to allow this capacity. It might be reasonable for a covered entity with a highly computerized information system to implement a system under which employees with certain functions have access to only limited fields in a patient records, while other employees have access to the complete records. Such a system might not be reasonable for a covered entity with a largely paper records system.

Covered entities' policies and procedures must provide that disclosure of an entire medical record will not be made except pursuant to policies which specifically justify why the entire medical record is needed.

We believe that these modifications significantly improve the workability of this standard. At the same time, we believe that asking covered entities to assess their practices and establish rules for themselves will lead to significant improvements in the privacy of health information. See the preamble for § 164.514 for a more detailed discussion.

Comment: The minimum necessary standard should not be applied to uses and disclosures for payment or health care operations.

Response: Commenter's arguments for exempting these uses and disclosures from the minimum necessary standard were not compelling. We believe that our modifications to application of the minimum necessary standard to internal uses of protected health information, and to routine disclosures, address many of the concerns raised, particularly the concerns about administrative burdens and the concerns about having the information necessary for day-to-day operations. We do not eliminate this standard in part because we also remain concerned that covered entities may be tempted to disclose an entire medical record when only a few items of information are necessary, to avoid the administrative step of extracting the necessary information (or redacting the unnecessary information). We also believe this standard will cause covered entities to assess their privacy practices, give the privacy interests of their patients and enrollees greater attention, and make improvements that might otherwise not have been made. For this reason, the privacy benefits of retaining the minimum necessary standard for these purposes outweigh the burdens involved. We note that the minimum necessary standard is tied to the purpose of the disclosure; thus, providers may disclose protected health information as necessary to obtain payment.

Comment: Other commenters urged us to apply a ''good faith'' provision to all disclosures subject to the minimum necessary standard. Commenters presented a range of options to modify the proposed provisions which, in their view, would have mitigated their liability if they failed to comply with minimum necessary standard.

Response: We believe that the modifications to this standard, described above, substantially address these commenters' concerns. In addition to allowing the covered entity to use standard protocols for routine disclosures, we modify the standard to require a covered entity to make ''reasonable efforts,'' not ''all'' reasonable efforts as proposed, in making the ''minimum necessary'' disclosure.

Comments: Some commenters complained that language in the proposed rule was vague and provided little guidance, and should be abandoned.

Response: In the preamble for § 164.504 and these responses to comments, we provide further guidance on how a covered entity can develop its policies for the minimum necessary use and disclosure of protected health information. We do not abandon this standard for the reasons described above. We remain concerned about the number of persons who have access to identifiable health information, and believe that causing covered entities to examine their practices will have significant privacy benefits.

Comment: Some commenters asked that the minimum necessary standard should not be applied to disclosures to business partners. Many of these commenters articulated the burdens they would bear if every disclosure to a business partner was required to meet the minimum necessary standard.

Response: We do not agree. In this final rule, we minimize the burden on covered entities in the following ways: in circumstances where disclosures are made on a routine, recurring basis, such as in on-going relationships between covered entities and their business associates, individual review of each routine disclosure has been eliminated; covered entities are required only to develop standard protocols to apply to such routine disclosures made to business associates (or types of business associates). In addition, we allow covered entities to rely on the representation of a professional hired to provide professional services as to what information is the minimum necessary for that purpose.

Comment: Some commenters were concerned that applying the standard in research settings will result in providers declining to participate in research protocols.

Response: We have modified the proposal to reduce the burden on covered entities that wish to disclose protected health information for research purposes. The final rule requires covered entities to obtain documentation or statements from persons requesting protected health information for research that, among other things, describe the information necessary for the research. We allow covered entities to reasonably rely on the documentation or statements as describing the minimum necessary disclosure.

Comment: Some commenters argued that government requests should not be subject to the minimum necessary standard, whether or not they are ''authorized by law.''

Response: We found no compelling reason to exempt government requests from this standard, other than when a disclosure is required by law. (See preamble to § 164.512(a) for the

rationale behind this policy). When a disclosure is required by law, the minimum necessary standard does not apply, whether the recipient of the information is a government official or a private individual.

At the same time, we understand that when certain government officials make requests for protected health information, some covered entities might feel pressure to comply that might not be present when the request is from a private individuals. For this reason, we allow (but do not require) covered entities to reasonably rely on the representations of public officials as to the minimum necessary information for the purpose.

Comment: Some commenters argued that requests under proposed § 164.510 should not be subject to the minimum necessary standard, whether or not they are ''authorized by law.'' Others argued that for disclosures made for administrative proceedings pursuant to proposed § 164.510, the minimum necessary standard should apply unless they are subject to a court order.

Response: We found no compelling reason to exempt disclosures for purposes listed in the regulation from this standard, other than for disclosures required by law. When there is no such legal mandate, the disclosure is voluntary on the part of the covered entity, and it is therefore reasonable to expect the covered entity to make some effort to protect privacy before making such a disclosure. If the covered entity finds that redacting unnecessary information, or extracting the requested information, prior to making the disclosure, is too burdensome, it need not make the disclosure. Where there is ambiguity regarding what information is needed, some effort on the part of the covered entity can be expected in these circumstances.

We also found no compelling reason to limit the exemption for disclosures ''required by law'' to those made pursuant to a court order. The judgment of a state legislature or regulatory body that a disclosure is required is entitled to no less deference than the same decision made by a court. For further rationale for this policy, see the preamble to § 164.512(a).

Comment: Some commenters argued that, in cases where a request for disclosure is not required by law, covered entities should be permitted to rely on the representations by public officials, that they have requested no more than the minimum amount necessary.

Response: We agree, and retain the proposed provision which allows reasonable reliance on the representations of public officials.

Comment: Some commenters argued that it is inappropriate to require covered entities to distinguish between disclosures that are ''required by law'' and those that are merely ''authorized by law,'' for the purposes of determining when the standard applies.

Response: We do not agree. Covered entities have an independent duty to be aware of their legal obligations to federal, state, local and territorial or tribal authorities. In addition, § 164.514(h) allows covered entities to reasonably rely on the oral or written representation of public officials that a disclosure is required by law.

Comment: The minimum necessary standard should not be applied to pharmacists, or to emergency services.

Response: We believe that the final rule's exemption of disclosures of protected health information to health care providers for treatment purposes from the minimum necessary standard addresses these commenters concerns about emergency services. Together with the other changes we make to the proposed standard, we believe we have also addressed most of the commenters' concerns about pharmacists. With respect to pharmacists, the comments offered no persuasive reasons to treat pharmacists differently from other health care providers. Our reasons for retaining this standard for other uses and disclosures of protected health information are explained above.

Comment: A number of commenters argued that the standard should not apply to disclosures to attorneys, because it would interfere with the professional duties and judgment of attorneys in their representation of covered entities. Commenters stated that if a layperson within a covered entity makes an improper decision as to what the minimum necessary information is in regard to a request by the entity's attorney, the attorney may end up lacking information that is vital to representation. These commenters stated that attorneys are usually going to be in a better position to determine what information is truly the minimum necessary for effective counsel and representation of the client.

Response: We found no compelling reason to treat attorneys differently from other business associates. However, to ensure that this rule does not inadvertently cause covered entities to second-guess the professional judgment of the attorneys and other professionals they hire, we modify the proposed policies to explicitly allow covered entities to rely on the representation of a professional hired to provide professional services as to what information is the minimum necessary for that purpose.

Comment: Commenters from the law enforcement community expressed concern that providers may attempt to misuse the minimum necessary standard as a means to restrict access to information, particularly with regard to disclosures for health oversight or to law enforcement officials.

Response: The minimum necessary standard does not apply to disclosures required by law. Since the disclosures to law enforcement officials to which this standard applies are all voluntary, there would be no need for a covered entity to ''manipulate'' the standard; it could decline to make the disclosure.

Comment: Some commenters argued that the only exception to the application of the standard should be when an individual requests access to his or her own information. Many of these commenters expressed specific concerns about victims of domestic violence and other forms of abuse.

Response: We do not agree with the general assertion that disclosure to the individual is the only appropriate exception to the minimum necessary standard. There are other, limited, circumstances in which application of the minimum necessary standard could cause significant harm. For reasons described above, disclosures of protected health information for treatment purposes are not subject to this standard. Similarly, as described in detail in the preamble to § 164.512(a), where another public body has mandated the disclosure of health information, upsetting that judgment in this regulation would not be appropriate.

The more specific concerns expressed about victims of domestic violence and other forms of abuse are addressed in a new provision regarding disclosure of protected health information related to domestic violence and abuse (see § 164.512(c)), and in new limitations on disclosures to persons involved in the individual's care (see § 164.510(b)). We believe that the limitations we place on disclosure of health information in those circumstances address the concerns of these commenters.

Comment: Some commenters argued that disclosures to next of kin should be restricted to minimum necessary protected health information, and to protected health information about only the current medical condition.

Response: In the final regulation, we change the proposed provision regarding ''next of kin'' to more clearly focus on the disclosures we intended to target: Disclosures to persons involved

in the individual's care. We allow such disclosure only with the agreement of the individual, or where the covered entity has offered the individual the opportunity to object to the disclosure and the individual did not object. If the opportunity to object cannot practicably be provided because of the incapacity of the individual or other emergency, we require covered entities to exercise professional judgment in the best interest of the patient in deciding whether to disclose information. In such cases, we permit disclosure only of that information directly relevant to the person's involvement with the individual's health care. (This provision also includes limited disclosure to certain persons seeking to identify or locate an individual.) See § 164.510(b).

Some additional concerns expressed about victims of domestic violence and other forms of abuse are also addressed in a new section on disclosure of protected health information related to domestic violence and abuse. See § 164.512(c). We believe that the limitations we place on disclosure of health information in these provisions address the concerns of these commenters.

Comment: Some commenters argued that covered entities should be required to determine whether de-identified information could be used before disclosing information under the minimum necessary standard.

Response: We believe that requiring covered entities' policies and procedures for minimum necessary disclosures to address whether de-identified information could be used in all instances would impose burdens on some covered entities that could outweigh the benefits of such a requirement. There is significant variation in the sophistication of covered entities' information systems. Some covered entities can reasonably implement policies and procedures that make significant use of de-identified information; other covered entities would find such a requirement excessively burdensome. For this reason, we chose instead to require ''reasonable efforts,'' which can vary according to the situation of each covered entity.

In addition, we believe that the fact that we allow de-identified information to be disclosed without regard to the policies, procedures, and documentation required for disclosure of identifiable health information will provide an incentive to encourage its use where appropriate.

Comment: Several commenters argued that standard transactions should not be subject to the standard.

Response: We agree that data elements that are required or situationally required in the standard transactions should not be, and are not, subject to this standard. However, in many cases, covered entities have significant discretion as to the information included in these transactions. Therefore, this standard does apply to those optional data elements.

Comment: Some commenters asked for clarification to understand how the minimum necessary standard is intended to interact with the security NPRM.

Response: The proposed Security Rule included requirements for electronic health information systems to include access management controls. Under this regulation, the covered entity's privacy policies will determine who has access to what protected health information. We will make every effort to ensure consistency prior to publishing the final Security Rule.

Comment: Many commenters, representing health care providers, argued that if the request was being made by a health plan, the health plan should be required to request only the minimum protected health information necessary. Some of these commenters stated that the requestor is in a better position to know the minimum amount of information needed for their purposes. Some of these commenters argued that the minimum necessary standard should be imposed only on the requesting entity. A few of these commenters argued that both the disclosing and the requesting entity should be subject to the minimum necessary standard, to create ''internal tension'' to assure the standard is honored.

Response: We agree, and in the final rule we require that a request for protected health information made by one covered entity to another covered entity must be limited to the minimum amount necessary for the purpose. As with uses and disclosures of protected health information, covered entities may have standard protocols for routine requests. Similarly, this requirement does not apply to requests made to health care providers for treatment purposes. We modify the rule to balance this provision; that is, it now applies both to disclosure of and requests for protected health information. We also allow, but do not require, the covered entity releasing the information to reasonably rely on the assertion of a requesting covered entity that it is requesting only the minimum protected health information necessary.

Comment: A few commenters suggested that there should be a process for resolving disputes between covered entities over what constitutes the ''minimum necessary'' information.

Response: We do not intend that this rule change the way covered entities currently handle their differences regarding the disclosure of health information. We understand that the scope of information requested from providers by health plans is a source of tension in the industry today, and we believe it would not be appropriate to use this regulation to affect that debate. As discussed above, we require both the requesting and the disclosing covered entity to take privacy concerns into account, but do not inject additional tension into the on-going discussions.

Section 164.514(e)—Marketing

Comment: Many commenters requested clarification of the boundaries between treatment, payment, health care operations, and marketing. Some of these commenters requested clarification of the apparent inconsistency between language in proposed § 164.506(a)(1)(i) (a covered entity is permitted to use or disclose protected health information without authorization ''to carry out'' treatment, payment, or health care operations) and proposed § 164.508(a)(2)(A) (a covered entity must obtain an authorization for all uses and disclosures that are not ''compatible with or directly related to'' treatment, payment, and health care operations). They suggested retaining the language in proposed § 164.508(a)(2)(A), which would permit a broader range of uses and disclosures without authorization, in order to engage in health promotion activities that might otherwise be considered marketing.

Response: In the final rule, we make several changes to the definitions of treatment, payment, and health care operations that are intended to clarify the uses and disclosures of protected health information that may be made for each purpose. See § 164.501 and the corresponding preamble discussion regarding the definitions of these terms. We also have added a definition of the term ''marketing'' to help establish the boundary between marketing and treatment, payment, and health care operations. See § 164.501. We also clarify the conditions under which authorization is or is not required for uses and disclosures of protected health information for marketing purposes. See § 164.514(e). Due to these changes, we believe it is appropriate to retain the wording from proposed § 164.506(a)(1)(i).

Comment: We received a wide variety of suggestions with respect to authorization for uses and disclosures of protected health information for marketing purposes. Some commenters supported requiring authorization for all such uses and disclosures. Other commenters suggested permitting all such uses and disclosures without authorization.

Some commenters suggested we distinguish between marketing to benefit the covered entity and marketing to benefit a third party. For example, a few commenters suggested we should prohibit covered entities from seeking authorization for any use or disclosure for marketing purposes that benefit a third party. These commenters argued that the third parties should be required to obtain the individual's authorization directly from the individual, not through a covered entity, due to the potential for conflicts of interest.

While a few commenters suggested that we require covered entities to obtain authorization to use or disclose protected health information for the purpose of marketing its own products and services, the majority argued these types of marketing activities are vital to covered entities and their customers and should therefore be permitted to occur without authorization. For example, commenters suggested covered entities should be able to use and disclose protected health information without authorization in order to provide appointment reminders, newsletters, information about new initiatives, and program bulletins.

Finally, many commenters argued we should not require authorization for the use or disclosure of protected health information to market any health-related goods and services, even if those goods and services are offered by a third party. Some of these commenters suggested that individuals should have an opportunity to opt out of these types of marketing activities rather than requiring authorization.

Response: We have modified the final rule in ways that address a number of the issues raised in the comments. First, the final rule defines the term marketing, and excepts certain communications from the definition. See § 164.501. These exceptions include communications made by covered entities for the purpose of describing network providers or other available products, services, or benefits and communications made by covered entities for certain treatment-related purposes. These exceptions only apply to oral communications or to written communications for which the covered entity receives no third-party remuneration. The exceptions to the definition of marketing fall within the definitions of treatment and/or health care operations, and therefore uses, or disclosures to a business associate, of protected health information for these purposes are permissible under the rule without authorization.

The final rule also permits covered entities to use protected health information to market health-related products and services, whether they are the products and services of the covered entity or of a third party, subject to a number of limitations. See § 164.514(e). We permit these uses to allow entities in the health sector to inform their patients and enrollees about products that may benefit them. The final rule contains significant restrictions, including requirements that the covered entity disclose itself as the source of a marketing communication, that it disclose any direct or indirect remuneration from third parties for making the disclosure, and that, except in the cases of general communications such as a newsletter, the communication disclose how the individual can opt-out of receiving additional marketing communications. Additional requirements are imposed if the communication is targeted based on the health status or condition of the proposed recipients.

We believe that these modifications address many of the issues raised by commenters and provide a substantial amount of flexibility as to when a covered entity may communicate about a health-related product or service to a patient or enrollee. These communications may include appointment reminders, newsletters, and information about new health products. These changes, however, do not permit a covered entity to disclose protected health information to third parties for marketing (other than to a business associate to make a marketing communication on behalf of the covered entity) without authorization under § 164.508.

Comment: A few commenters suggested we prohibit health care clearinghouses from seeking authorization for the use or disclosure of protected health information for marketing purposes.

Response: We do not prohibit clearinghouses from seeking authorizations for these purposes. We believe, however, that health care clearinghouses will almost always create or obtain protected health information in a business associate capacity. Business associates may only engage in activities involving the use or disclosure of protected health information, including seeking or acting on an authorization, to the extent their contracts allow them to do so. When a clearinghouse creates or receives protected health information other than as a business associate of a covered entity, it is permitted and required to obtain authorizations to the same extent as any other covered entity.

Comment: A few commenters suggested we require covered entities to publicly disclose, on the covered entity's website or upon request, all of their marketing arrangements.

Response: While we agree that such a requirement would provide individuals with additional information about how their information would be used, we do not feel that such a significant intrusion into the business practices of the covered entity is warranted.

Comment: Some commenters argued that if an activity falls within the scope of payment, it should not be considered marketing. Commenters strongly supported an approach which would bar an activity from being construed as ''marketing'' even if performing that activity would result in financial gain to the covered entity. In a similar vein, we were urged to adopt the position that if an activity was considered payment, treatment or health care operations, it could not be further evaluated to determine whether it should be excluded as marketing.

Response: We considered the approach offered by commenters but decided against it. Some activities, such as the marketing of a covered entity's own health-related products or services, are now included in the definition of health care operations, provided certain requirements are met. Other types of activities, such as the sale of a patient list to a marketing firm, would not be permitted under this rule without authorization from the individual. We do not believe that we can envision every possible disclosure of health information that would violate the privacy of an individual, so any list would be incomplete. Therefore, whether or not a particular activity is considered marketing, payment, treatment or health care operations will be a fact-based determination based on the activity's congruence with the particular definition.

Comment: Some industry groups stated that if an activity involves selling products, it is not disease management. They suggested we adopt a definition of disease management that differentiates use of information for the best interests of patient from uses undertaken for ''ulterior purposes'' such as advertising, marketing, or promoting separate products.

Response: We agree in general that the sale of unrelated products to individuals is not a population-based activity that supports treatment and payment. However, in certain circumstances marketing activities are permitted as a health care operation; see the definition of ''health care operations'' in § 164.501 and the related marketing requirements of § 164.514.

Comment: Some commenters complained that the absence of a definition for disease management created uncertainty, in view of the proposed rule's requirement to get authorization for marketing. They expressed concern that the effect would be to require patient consent for many activities that are desirable, not practicably done if authorization is required, and otherwise classifiable as treatment, payment, or health care operations. Examples provided include reminders for appointments, reminders to get preventive services like mammograms, and information about home management of chronic illnesses. They also stated that the proposed rule would prevent many disease management and preventive health activities.

Response: We agree that the distinction in the NPRM between disease management and marketing was unclear. Rather than provide a definition of disease management, this final rule defines marketing. We note that overlap between disease management and marketing exists today in practice and they cannot be distinguished easily with a definitional label. However, for purposes of this rule, the revised language makes clear for what activities an authorization is required. We note that under this rule many of the activities mentioned by commenters will not require authorizations under most circumstances. See the discussion of disease management under the definition of ''treatment'' in § 164.501.

Section 164.514(f)—Fundraising

Comment: Many comments objected to the requirement that an authorization from the individual be obtained for use and disclosure of protected health information for fundraising purposes. They argued that, in the case of not-for-profit health care providers, having to obtain authorization would be time consuming and costly, and that such a requirement would lead to a decrease in charitable giving. The commenters also urged that fundraising be included within the definition of health care operations. Numerous commenters suggested that they did not need unfettered access to patient information in order to carry out their fundraising campaigns. They stated that a limited data set restricted to name, address, and telephone number would be sufficient to meet their needs. Several commenters suggested that we create a voluntary opt-out provision so people can avoid solicitations.

Response: We agree with commenters that our proposal could have adversely effected charitable giving, and accordingly make several modifications to the proposal. First, the final rule allows a covered entity to use or disclose to a business associate protected health information without authorization to identify individuals for fundraising for its own benefit. Permissible fundraising activities include appeals for money, sponsorship of events, etc. They do not include royalties or remittances for the sale of products of third parties (except auctions, rummage sales, etc).

Second, the final rule allows a covered entity to disclose protected health information without authorization to an institutionally related foundation that has as its mission to benefit the covered entity. This special provision is necessary to accommodate tax code provisions which may not allow such foundations to be business associates of their associated covered entity.

We also agree that broad access to protected health information is unnecessary for fundraising and unnecessarily intrudes on individual privacy. The final rule limits protected health information to be used or disclosed for fundraising to demographic information and the date that treatment occurred. Demographic information is not defined in the rule, but will generally include in this context name, address and other contact information, age, gender, and insurance status. The term does not include any information about the illness or treatment.

We also agree that a voluntary opt-out is an appropriate protection, and require in § 164.520 that covered entities provide information on their fundraising activities in their ''Notice of Information Practices.'' As part of the notice and in any fundraising materials, covered entities must provide information explaining how individuals may opt out of fundraising communications.

Comment: Some commenters stated that use and disclosure of protected health information for fundraising, without authorization should be limited to not-for-profit entities. They suggested that not-for-profit entities were in greater need of charitable contributions and as such, they should be exempt from the authorization requirement while for-profit organizations should have to comply with the requirement.

Response: We do not agree that the profit status of a covered entity should determine its allowable use of protected health information for fundraising. Many for-profit entities provide the same services and have similar missions to not-for-profit entities. Therefore, the final rule does not make this distinction.

Comment: Several commenters suggested that the final rule should allow the internal use of protected health information for fundraising, without authorization, but not disclosure for fundraising. These commenters suggested that by limiting access of protected health information to only internal development offices concerns about misuse would be reduced.

Response: We do not agree. A number of commenters noted that they have related charitable foundations that raise funds for the covered entity, and we permit disclosures to such foundations to ensure that this rule does not interfere with charitable giving.

Comment: Several commenters asked us to address the content of fundraising letters. They pointed out that disease or condition-specific letters requesting contributions, if opened by the wrong person, could reveal personal information about the intended recipient.

Response: We agree that such communications raise privacy concerns. In the final rule, we limit the information that can be used or disclosed for fundraising, and exclude information about diagnosis, nature of services, or treatment.

Section 164.514(g)—Verification

Comment: A few commenters suggested that verification guidelines may need to be different as they apply to emergency clinical situations as opposed to routine data collection where delays do not threaten health.

Response: We agree, and make special provisions in §§ 164.510 and 164.512 for disclosures of protected health information by a covered entity without authorization where the individual is unable to agree or object to disclosure due to incapacity or other emergency circumstance.

For example, a health care provider may need to make disclosures to family members, close personal friends, and others involved in the individual's care in emergency situations. Similarly, a health care provider may need to respond to a request from a hospital seeking protected health information in

a circumstance described as an emergency. In each case, we require only that the covered entity exercise professional judgment, in the best interest of the patient, in deciding whether to make a disclosure. Based on the comments and our fact finding, this reflects current practice.

Comment: A few commenters stated the rules should include provisions for electronic verification of identity (such as Public Key Infrastructure (PKI)) as established in the regulations on Security and Electronic Signatures. One commenter suggested that some kind of PKI credentialing certificate should be required.

Response: This regulation does not address specific technical protocols utilized to meet the verification requirements. If the requirements of the rule are otherwise met, the mechanism for meeting them can be determined by the covered entity.

Comment: A few commenters wanted more clarification on the verification procedures. One commenter wanted to know if contract number is enough for verification. A few commenters wanted to know if a callback or authorization on a letterhead is acceptable. A few commenters wanted to know if plans are considered to ''routinely do business'' with all of their members.

Response: In the final rule, we modify the proposed provision and require covered entities to have policies and procedures reasonably designed to verify the identify and authority of persons requesting protected health information. Whether knowledge of a contract number is reasonable evidence of authority and identity will depend on the circumstances. Call-backs and letterhead are typically used today for verification, and are acceptable under this rule if reasonable under the circumstances. For communications with health plan members, the covered entity will already have information about each individual, collected during enrollment, that can be used to establish identity, especially for verbal or electronic inquiries. For example, today many health plans ask for the social security or policy number of individuals seeking information or assistance by telephone. How this verification is done is left up to the covered entity.

Comment: One commenter expressed the need for consistency on verification requirements between this rule and the Security regulation.

Response: We will make every effort to ensure consistency prior to publishing the final Security Rule.

Comment: One commenter stated that the verification language in proposed § 164.518(c)(2)(ii)(B)(1) would have created a presumption that ''a request for disclosure made by official legal process issued by a[n] administrative body'' is reasonable legal authority to disclose the protected health information. The commenter was concerned that this provision could be interpreted to permit a state agency to demand the disclosure of protected health information merely on the basis of a letter signed by an agency representative. The commenter believed that the rule specifically should defer to state or federal law on the disclosure of protected health information pursuant to legal process.

Response: The verification provisions in this rule are minimum requirements that covered entities must meet before disclosing protected health information under this regulation. They do not mandate disclosure, nor do they preempt state laws which impose additional restrictions on disclosure. Where state law regarding disclosures is more stringent, the covered entity must adhere to state law.

Comment: A few commenters wanted the verification requirements to apply to disclosures of protected health information for treatment, payment and operations purposes.

Response: We agree. This verification requirement applies to all disclosures of protected health information permitted by this rule, including for treatment, payment and operations, where the identity of the recipient is not known to the covered entity. Routine communications between providers, where existing relationships have been established, do not require special verification procedures.

Comment: A few commenters were concerned that a verbal inquiry for next of kin verification is not consistent with the verification guidelines of this verification subsection and that verbal inquiry would create problems because anyone who purports to be a next of kin could easily obtain information under false pretenses.

Response: In the final rule in § 164.514, we require the covered entity to verify the identity and authority of persons requesting protected health information, where the identity and authority of such person is not known to the covered entity. This applies to next of kin situations. Procedures for disclosures to next of kin, other family members and persons assisting in an individual's care are also discussed in § 164.510(b), which allows the covered entity to exercise professional judgment as to whether the disclosure is in the individual's best interest when the individual is not available to agree to the disclosure or is incapacitated. Requiring written proof of identity in many of these situations, such as when a family member is seeking to locate a relative in an emergency or disaster situation, would create enormous burden without a corresponding enhancement of privacy, and could cause unnecessary delays in these situations. We therefore believe that reliance on professional judgment provides a better framework for balancing the need for privacy with the need to locate and identify individuals.

Comment: A few commenters stated that the verification requirements will provide great uncertainty to providers who receive authorizations from life, disability income and long-term care insurers in the course of underwriting and claims investigation. They are unaware of any breaches of confidentiality associated with these circumstances and believe the rule creates a solution to a non-existent problem. Another commenter stated that it is too burdensome for health care providers to verify requests that are normally received verbally or via fax.

Response: This rule requires covered health care providers to adhere to current best practices for verification. That is, when the requester is not known to the covered provider, the provider makes a reasonable effort to determine that the protected health information is being sent to the entity authorized to receive it. Our fact finding reveals that this is often done by sending the information to a recognizable organizational address or if being transmitted by fax or phone by calling the requester back through the main organization switchboard rather than through a direct phone number. We agree that these procedures seem to work reasonably well in current practice and are sufficient to meet the relevant requirements in the final rule.

Comments: One comment suggested requiring a form of photo identification such as a driver's license or certain personal information such as date of birth to verify the identity of the individual.

Response: These are exactly the types of standard procedures for verifying the identity of individuals that are envisioned by the final rule. Most health care entities already conduct such procedures successfully. However, it is unwise to prescribe specific means of verification for all situations. Instead, we require policies and procedures reasonably designed for purposes of verification.

Comment: One professional association said that the example procedure described in the NPRM for asking questions to verify that an adult

acting for a young child had the requisite relationship to the child would be quite complex and difficult in practice. The comment asked for specific guidance as to what questions would constitute an adequate attempt to verify such a relationship.

Response: The final rule requires the covered entity to implement policies and procedures that are reasonably designed to comply with the verification requirement in § 164.514. It would not be possible to create the requested specific guidance which could deal with the infinite variety of situations that providers must face, especially the complex ones such as that described by the commenter. As with many of the requirements of this final rule, health care providers are given latitude and expected to make decisions regarding disclosures, based on their professional judgment and experience with common practice, in the best interest of the individual.

Comment: One commenter asserted that ascertaining whether a requestor has the appropriate legal authority is beyond the scope of the training or expertise of most employees in a physician's office. They believe that health care providers must be able to reasonably rely on the authority of the requestor.

Response: In the final regulation we require covered entities to have policies and procedures reasonably designed to verify the identify and authority of persons requesting health information. Where the requester is a public official and legal authority is at issue, we provide detailed descriptions of the acceptable methods for such verification in the final rule. For others, the covered entity must implement policies and procedures that are reasonably designed to comply with the requirement to verify the identity and authority of a requestor, but only if the requestor is unknown to the covered entity. As described above, we expect these policies and procedures to document currently used best practices and reliance on professional judgment in the best interest of the individual.

Comment: One commenter expressed concern that the verification/identification procedures may eliminate or significantly reduce their ability to utilize medical records copy services. As written, they believe the NPRM provides the latitude to set up copy service arrangements, but any change that would add restrictions would adversely affect their ability to process an individual's disability claim.

Response: The covered entity can establish reasonable policies and procedures to address verification in routine disclosures under business associate agreements, with, for example, medical records copy services. Nothing in the verification provisions would preclude those activities, nor have we significantly modified the NPRM provision on this issue.

Section 164.520—Notice of Privacy Practices for Protected Health Information

Comment: Many commenters supported the proposal to require covered entities to produce a notice of information practices. They stated that such notice would improve individuals' understanding of how their information may be used and disclosed and would help to build trust between individuals and covered entities. A few comments, however, argued that the notice requirement would be administratively burdensome and expensive without providing significant benefit to individuals.

Response: We retain the requirement for covered health care providers and health plans to produce a notice of information practices. We additionally require health care clearinghouses that create or receive protected health information other than as a business associate of another covered entity to produce a notice. We believe the notice will provide individuals with a clearer understanding of how their information may be used and disclosed and is essential to inform individuals of their privacy rights. The notice will focus individuals on privacy issues, and prompt individuals to have discussions about privacy issues with their health plans, health care providers, and other persons.

The importance of providing individuals with notice of the uses and disclosures of their information and of their rights with respect to that information is well supported by industry groups, and is recognized in current state and federal law. The July 1977 Report of the Privacy Protection Study Commission recommended that ''each medical-care provider be required to notify an individual on whom it maintains a medical record of the disclosures that may be made of information in the record without the individual's express authorization.'' [23] The Commission also recommended that ''an insurance institution * * * notify (an applicant or principal insured) as to: * * * the types of parties to whom and circumstances under which information about the individual may be disclosed without his authorization, and the types of information that may be disclosed; [and] * * * the procedures whereby the individual may correct, amend, delete, or dispute any resulting record about himself.'' [24] The Privacy Act (5 U.S.C. 552a) requires government agencies to provide notice of the routine uses of information the agency collects and the rights individuals have with respect to that information. In its report ''Best Principles for Health Privacy,'' the Health Privacy Working Group stated, ''Individuals should be given notice about the use and disclosure of their health information and their rights with regard to that information.'' [25] The National Association of Insurance Commissioners' Health Information Privacy Model Act requires carriers to provide a written notice of health information policies, standards, and procedures, including a description of the uses and disclosures prohibited and permitted by the Act, the procedures for authorizing and limiting disclosures and for revoking authorizations, and the procedures for accessing and amending protected health information.

Some states require additional notice. For example, Hawaii requires health care providers and health plans, among others, to produce a notice of confidentiality practices, including a description of the individual's privacy rights and a description of the uses and disclosures of protected health information permitted under state law without the individual's authorization. (HRS section 323C–13)

Today, health plan hand books and evidences of coverage include some of what is required to be in the notice. Industry and standard-setting organizations have also developed notice requirements. The National Committee for Quality Assurance accreditation guidelines state that an accredited managed care organization ''communicates to prospective members its policies and practices regarding the collection, use, and disclosure of medical information [and] * * * informs members * * * of its policies and procedures on * * * allowing members access to their medical records.'' [26] Standards of the American Society for Testing and Materials state,

[23] Privacy Protection Study Commission, ''Personal Privacy in an Information Society,'' July 1977, p. 313.

[24] Privacy Protection Study Commission, ''Personal Privacy in an Information Society,'' July 1977, p. 192.

[25] Health Privacy Working Group, ''Best Principles for Health Privacy,'' Health Privacy Project, Institute for Health Care Research and Policy, Georgetown University, July 1999, p.19.

[26] National Committee on Quality Assurance, ''Surveyor Guidelines for the Accreditation of MCOs,'' effective July 1, 2000—June 30, 2001, p. 324.

''Organizations and individuals who collect, process, handle, or maintain health information should provide individuals and the public with a notice of information practices.'' They recommend that the notice include, among other elements, ''a description of the rights of individuals, including the right to inspect and copy information and the right to seek amendments [and] a description of the types of uses and disclosures that are permitted or required by law without the individual's authorization.'' [27] We build on this well-established principle in this final rule.

Comment: We received many comments on the model notice provided in the proposed rule. Some commenters argued that patients seeing similar documents would be less likely to become disoriented when examining a new notice. Other commenters, however, opposed the inclusion of a model notice or expressed concern about particular language included in the model. They maintained that a uniform model notice would never capture the varying practices of covered entities. Many commenters opposed requirements for a particular format or specific language in the notice. They stated that covered entities should be afforded maximum flexibility in fashioning their notices. Other commenters requested inclusion of specific language as a header to indicate the importance of the notice. A few commenters recommended specific formatting requirements, such as font size or type.

Response: On the whole, we found commenters' arguments for flexibility in the regulation more persuasive than those arguing for more standardization. We agree that a uniform notice would not capture the wide variation in information practices across covered entities. We therefore do not include a model notice in the final rule, and do not require inclusion of specific language in the notice (except for a standard header). We also do not require particular formatting. We do, however, require the notice to be written in plain language. (See above for guidance on writing documents in plain language.) We also agree with commenters that the notice should contain a standard header to draw the individual's attention to the notice and facilitate the individual's ability to recognize the notice across covered entities.

We believe that post-publication guidance will be a more effective mechanism for helping covered entities design their notices than the regulation itself. After the rule is published, we can provide guidance on notice content and format tailored to different types of health plans and providers. We believe such specially designed guidance will be more useful than a one-size-fits-all model notice we might publish with this regulation.

Comment: Commenters suggested that the rule should require that the notice regarding privacy practices include specific provisions related to health information of unemancipated minors.

Response: Although we agree that minors and their parents should be made aware of practices related to confidentiality of protected health information of unemancipated minors, we do not require covered entities that treat minors or use their protected health information to include provisions in their notice that are not required of other covered entities. In general, the content of notice requirements in § 164.520(b) do not vary based on the status of the individual being served. We have decided to maintain consistency by declining to prescribe specific notice requirements for minors. The rule does permit a covered entity to provide individuals with notice of its policies and procedures with respect to anticipated uses and disclosures of protected health information (§ 164.520(b)(2)), and providers are encouraged to do so.

Comment: Some commenters argued that covered entities should not be required to distinguish between those uses and disclosures that are required by law and those that are permitted by law without authorization, because these distinctions may not always be clear and will vary across jurisdictions. Some commenters maintained that simply stating that the covered entity would make all disclosures required by law would be sufficient. Other comments suggested that covered entities should be able to produce very broadly stated notices so that repeated revisions and mailings of those revisions would not be necessary.

Response: While we believe that covered entities have an independent duty to understand the laws to which they are subject, we also recognize that it could be difficult to convey such legal distinctions clearly and concisely in a notice. We therefore eliminate the proposed requirement for covered entities to distinguish between those uses and disclosures that are required by and those that are permitted by law. We instead require that covered entities describe each purpose for which they are permitted or required to use or disclose protected health information under this rule and other applicable law without individual consent or authorization. Specifically, covered entities must describe the types of uses and disclosures they are permitted to make for treatment, payment, and health care operations. They must also describe each of the purposes for which the covered entity is permitted or required by this subpart to use or disclose protected health information without the individual's written consent or authorization (even if they do not plan to make a permissive use or disclosure). We believe this requirement provides individuals with sufficient information to understand how information about them can be used and disclosed and to prompt them to ask for additional information to obtain a clearer understanding, while minimizing covered entities' burden.

A notice that stated only that the covered entity would make all disclosures required by law, as suggested by some of these commenters, would fail to inform individuals of the uses and disclosures of information about them that are permitted, but not required, by law. We clarify that each and every disclosure required by law need not be listed on the notice. Rather, the covered entity can include a general statement that disclosures required by law will be made.

Comment: Some comments argued that the covered entity should not have to provide notice about uses and disclosures that are permitted under the rule without authorization. Other comments suggested that the notice should inform individuals about all of the uses and disclosures that may be made, with or without the individual's authorization.

Response: When the individual's permission is not required for uses and disclosures of information, we believe providing the required notice is the most effective means of ensuring that individuals are aware of how information about them may be shared. The notice need not describe uses and disclosures for which the individual's permission is required, because the individual will be informed of these at the time permission to use or disclose the information is requested.

We additionally require covered entities, even those required to obtain the individual's consent for use and disclosure of protected health information for treatment, payment, and health care operations, to describe those uses and disclosures in their notice. (See § 164.506 and the corresponding preamble discussion regarding consent requirements.) We require these uses

[27] ASTM, ''Standard Guide for Confidentiality, Privacy, Access and Data Security, Principles for Health Information Including Computer-Based Patient Records,'' E 1869–97, § 9.2.

and disclosures to be described in the notice in part in order to reduce the administrative burden on covered providers that are required to obtain consent. Rather than obtaining a new consent each time the covered provider's information policies and procedures are materially revised, covered providers may revise and redistribute their notice. We also expect that the description of how information may be used to carry out treatment, payment, and health care operations in the notice will be more detailed than in the more general consent document.

Comment: Some commenters argued that covered entities should not be required to provide notice of the right to request restrictions, because doing so would be burdensome to the covered entity and distracting to the individual; because individuals have the right whether they are informed of such right or not; and because the requirement would be unlikely to improve patient care.

Response: We disagree. We believe that the ability of an individual to request restrictions is an important privacy right and that informing people of their rights improves their ability to exercise those rights. We do not believe that adding a sentence to the notice is burdensome to covered entities.

Comment: We received comments supporting inclusion of a contact point in the notice, so that individuals will not be forced to make multiple calls to find someone who can assist them with the issues in the notice.

Response: We retain the requirement, but clarify that the title of the contact person is sufficient. A person's name is not required.

Comment: Some commenters argued that we could facilitate compliance by requiring the notice to include the proposed requirement that covered entities use and disclose only the minimum necessary protected health information.

Response: We do not agree that adding such a requirement would strengthen the notice. The purpose of the notice is to inform individuals of their privacy rights, and of the purposes for which protected health information about them may be used or disclosed. Informing individuals that covered entities may use and disclose only the minimum necessary protected health information for a purpose would not increase individuals' understanding of their rights or the purposes for which information may be used or disclosed.

Comment: A few commenters supported allowing covered entities to apply changes in their information practices to protected health information obtained prior to the change. They argued that requiring different protections for information obtained at different times would be inefficient and extremely difficult to administer. Some comments supported requiring covered entities to state in the notice that the information policies and procedures are subject to change.

Response: We agree. In the final rule, we provide a mechanism by which covered entities may revise their privacy practices and apply those revisions to protected health information they already maintain. We permit, but do not require, covered entities to reserve the right to change their practices and apply the revised practices to information previously created or obtained. If a covered entity wishes to reserve this right, it must make a statement to that effect in its notice. If it does not make such a statement, the covered entity may still revise its privacy practices, but it may apply the revised practices only to protected health information created or obtained after the effective date of the notice in which the revised practices are reflected. See § 164.530(i) and the corresponding preamble discussion of requirements regarding changes to information policies and procedures.

Comment: Some commenters requested clarification of the term ''material changes'' so that entities will be comfortable that they act properly after making changes to their information practices. Some comments stated that entities should notify individuals whenever a new category of disclosures to be made without authorization is created.

Response: The concept of ''material change'' appears in other notice laws, such as the ERISA requirements for summary plan descriptions. We therefore retain the ''materiality'' condition for revision of notices, and encourage covered entities to draw on the concept as it has developed through those other laws. We agree that the addition of a new category of use or disclosure of health information that may be made without authorization would likely qualify as a material change.

Comment: We proposed to permit covered entities to implement revised policies and procedures without first revising the notice if a compelling reason existed to do so. Some commenters objected to this proposal because they were concerned that the ''compelling reason'' exception would give covered entities broad discretion to engage in post hoc violations of its own information practices.

Response: We agree and eliminate this provision. Covered entities may not implement revised information policies and procedures before properly documenting the revisions and updating their notice. See § 164.530(i). Because in the final rule we require the notice to include all disclosures that may be made, not only those the covered entity intends to make, we no longer need this provision to accommodate emergencies.

Comment: Some comments suggested that we require covered entities to maintain a log of all past notices, with changes from the previous notice highlighted. They further suggested we require covered entities to post this log on their web sites.

Response: In accordance with § 164.530(j)(2), a covered entity must retain for six years a copy of each notice it issues. We do not require highlighting of changes to the notice or posting of prior notices, due to the associated administrative burdens and the complexity such a requirement would build into the notice over time. We encourage covered entities, however, to make such materials available upon request.

Comment: Several commenters requested clarification about when, relative to the compliance date, covered entities are required to produce their notice. One commenter suggested that covered entities be allowed a period not less than 180 days after adoption of the final rule to develop and distribute the notice. Other comments requested that the notice compliance date be consistent with other HIPAA regulations.

Response: We require covered entities to have a notice available upon request as of the compliance date of this rule (or the compliance date of the covered entity if such date is later). See § 164.534 and the corresponding preamble discussion of the compliance date.

Comment: Some commenters suggested that covered entities, particularly covered health care providers, should be required to discuss the notice with individuals. They argued that posting a notice or otherwise providing the notice in writing may not achieve the goal of informing individuals of how their information will be handled, because some individuals may not be literate or able to function at the reading level used in the notice. Others argued that entities should have the flexibility to choose alternative modes of communicating the information in the notice, including voice disclosure. In contrast, some commenters were concerned that requirements to provide the notice in plain language or in languages other than English would be overly burdensome.

Response: We require covered entities to write the notice in plain language so that the average reader will be able to understand the notice. We encourage, but do not require, covered entities to consider alternative means of communicating with certain populations. We note that any covered entity that is a recipient of federal financial assistance is generally obligated under Title VI of the Civil Rights Act of 1964 to provide material ordinarily distributed to the public in the primary languages of persons with limited English proficiency in the recipients' service areas. While we believe the notice will prompt individuals to initiate discussions with their health plans and health care providers about the use and disclosure of health information, we believe this should be a matter left to each individual and that requiring covered entities to initiate discussions with each individual would be overly burdensome.

Comment: Some commenters suggested that covered entities, particularly health plans, should be permitted to distribute their notice in a newsletter or other communication with individuals.

Response: We agree, so long as the notice is sufficiently separate from other important documents. We therefore prohibit covered entities from combining the notice in a single document with either a consent (§ 164.506) or an authorization (§ 164.508), but do not otherwise prohibit covered entities from including the notice in or with other documents the covered entity shares with individuals.

Comment: Some comments suggested that covered entities should not be required to respond to requests for the notice from the general public. These comments indicated that the requirement would place an undue burden on covered entities without benefitting individuals.

Response: We proposed that the notice be publicly available so that individuals may use the notice to compare covered entities' privacy practices and to select a health plan or health care provider accordingly. We therefore retain the proposed requirement for covered entities to provide the notice to any person who requests a copy, including members of the general public.

Comment: Many commenters argued that the distribution requirements for health plans should be less burdensome. Some suggested requiring distribution upon material revision, but not every three years. Some suggested that health plans should only be required to distribute their notice annually or upon re-enrollment. Some suggested that health plans should only have to distribute their notice upon initial enrollment, not re-enrollment. Other commenters supported the proposed approach.

Response: We agree that the notice distribution requirements for health plans can be less burdensome than in the NPRM while still being effective. In the final rule, we reduce health plans' distribution burden in several ways. First, we require health plans to remind individuals every three years of the availability of the notice and of how to obtain a copy of the notice, rather than requiring the notice to be distributed every three years as proposed. Second, we clarify that health plans only have to distribute the notice to new enrollees on enrollment, not to current members of the health plan upon re-enrollment. Third, we specifically allow all covered entities to distribute the notice electronically in accordance with § 164.520(c)(3).

We retain the requirement for health plans to distribute the notice within 60 days of a material revision. We believe the revised distribution requirements will ensure that individuals are adequately informed of health plans' information practices and any changes to those procedures, without unduly burdening health plans.

Comment: Many commenters argued that health plans should not be required to distribute their notice to every person covered by the plan. They argued that distributing the notice to every family member would be unnecessarily duplicative, costly, and difficult to administer. They suggested that health plans only be required to distribute the notice to the primary participant or to each household with one or more insured individuals.

Response: We agree, and clarify in the final rule that a health plan may satisfy the distribution requirement by providing the notice to the named insured on behalf of the dependents of that named insured. For example, a group health plan may satisfy its notice requirement by providing a single notice to each covered employee of the plan sponsor. We do not require the group health plan to distribute the notice to each covered employee and to each covered dependent of those employees.

Comment: Many comments requested clarification about health plans' ability to distribute the notice via other entities. Some commenters suggested that group health plans should be able to satisfy the distribution requirement by providing copies of the notice to plan sponsors for delivery to employees. Others requested clarification that covered health care providers are only required to distribute their own notice and that health plans should be prohibited from using their affiliated providers to distribute the health plan's notice.

Response: We require health plans to distribute their notice to individuals covered by the health plan. Health plans may elect to hire or otherwise arrange for others, including group health plan sponsors and health care providers affiliated with the health plan, to carry out this distribution. We require covered providers to distribute only their own notices, and neither require nor prohibit health plans and health care providers from devising whatever arrangements they find suitable to meet the requirements of this rule. However, if a covered entity arranges for another person or entity to distribute the covered entity's notice on its behalf and individuals do not receive such notice, the covered entity would be in violation of the rule.

Comment: Some comments stated that covered providers without direct patient contact, such as clinical laboratories, might not have sufficient patient contact information to be able to mail the notice. They suggested we require or allow such providers to form agreements with referring providers or other entities to distribute notices on their behalf or to include their practices in the referring entity's own notice.

Response: We agree with commenters' concerns about the potential administrative and financial burdens of requiring covered providers that have indirect treatment relationships with individuals, such as clinical laboratories, to distribute the notice. Therefore, we require these covered providers to provide the notice only upon request. In addition, these covered providers may elect to reach agreements with other entities distribute their notice on their behalf, or to participate in an organized health care arrangement that produces a joint notice. See § 164.520(d) and the corresponding preamble discussion of joint notice requirements.

Comment: Some commenters requested that covered health care providers be permitted to distribute their notice prior to an individual's initial visit so that patients could review the information in advance of the visit. They suggested that distribution in advance would reduce the amount of time covered health care providers' staff would have to spend explaining the notice to patients in the office. Other comments argued that providers should

distribute their notice to patients at the time the individual visits the provider, because providers lack the administrative infrastructure necessary to develop and distribute mass communications and generally have difficulty identifying active patients.

Response: In the final rule, we clarify that covered providers with direct treatment relationships must provide the notice to patients no later than the first service delivery to the patient after the compliance date. For the reasons identified by these commenters, we do not require covered providers to send their notice to the patient in advance of the patient's visit. We do not prohibit distribution in advance, but only require distribution to the patient as of the time of the visit. We believe this flexibility will allow each covered provider to develop procedures that best meet its and its patients' needs.

Comment: Some comments suggested that covered providers should be required to distribute the notice as of the compliance date. They noted that if the covered provider waited to distribute the notice until first service delivery, it would be possible (pursuant to the rule) for a use or disclosure to be made without the individual's authorization, but before the individual receives the notice.

Response: Because health care providers generally lack the administrative infrastructure necessary to develop and distribute mass communications and generally have difficulty identifying active patients, we do not require covered providers to distribute the notice until the first service delivery after the compliance date. We acknowledge that this policy allows uses and disclosure of health information without individuals' consent or authorization before the individual receives the notice. We require covered entities, including covered providers, to have the notice available upon request as of the compliance date of the rule. Individuals may request a copy of the notice from their provider at any time.

Comment: Many commenters were concerned with the requirement that covered providers post their notice. Some commenters suggested that covered hospital-based providers should be able to satisfy the distribution requirements by posting their notice in multiple locations at the hospital, rather than handing the notice to patients—particularly with respect to distribution after material revisions have been made. Some additionally suggested that these covered providers should have copies of the notice available on site. Some commenters emphasized that the notice must be clear and conspicuous to give individuals meaningful and effective notice of their rights. Other commenters noted that posting the notice will not inform former patients who no longer see the provider.

Response: We clarify in the final rule that the requirement to post a notice does not substitute for the requirement to give individuals a notice or make notices available upon request. Covered providers with direct treatment relationships, including covered hospitals, must give a copy of the notice to the individual as of first service delivery after the compliance date. After giving the individual a copy of the notice as of that first visit, the covered provider has no other obligation to actively distribute the notice. We believe it is unnecessarily burdensome to require covered providers to mail the notice to all current and former patients each time the notice is revised, because unlike health plans, providers may have a difficult time identifying active patients. All individuals, including those who no longer see the covered provider, have the right to receive a copy of the notice on request.

If the covered provider maintains a physical delivery site, it must also post the notice (including revisions to the notice) in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered provider to be able to read the notice. The covered provider must also have the notice available on site for individuals to be able to request and take with them.

Comment: Some comments requested clarification about the distribution requirements for a covered entity that is a health plan and a covered health care provider.

Response: Under § 164.504(g), discussed above, covered entities that conduct multiple types of covered functions, such as the kind of entities described in the above comments, are required to comply with the provisions applicable to a particular type of health care function when acting in that capacity. Thus, in the example described above, the covered entity is required by § 164.504(g) to follow the requirements for health plans with respect to its actions as a health plan and to follow the requirements for health care providers with respect to its actions as a health care provider.

Comment: We received many comments about the ability of covered entities to distribute their notices electronically. Many commenters suggested that we permit covered entities to distribute the notice electronically, either via a web site or e-mail. They argued that covered entities are increasingly using electronic technology to communicate with patients and otherwise administer benefits. They also noted that other regulations permit similar documents, such as ERISA-required summary plan descriptions, to be delivered electronically. Some commenters suggested that electronic distribution should be permitted unless the individual specifically requests a hard copy or lacks electronic access. Some argued that entities should be able to choose a least-cost alternative that allows for periodic changes without excessive mailing costs. A few commenters suggested requiring covered entities to distribute notices electronically.

Response: We clarify in the final rule that covered entities may elect to distribute their notice electronically, provided the individual agrees to receiving the notice electronically and has not withdrawn such agreement. We do not require any particular form of agreement. For example, a covered provider could ask an individual at the time the individual requests a copy of the notice whether she prefers to receive it in hard copy or electronic form. A health plan could ask an individual applying for coverage to provide an e-mail address where the health plan can send the individual information. If the individual provides an e-mail address, the health plan can infer agreement to obtain information electronically.

An individual who has agreed to receive the notice electronically, however, retains the right to request a hard copy of the notice. This right must be described in the notice. In addition, if the covered entity knows that electronic transmission of the notice has failed, the covered entity must produce a hard copy of the notice. We believe this provision allows covered entities flexibility to provide the notice in the form that best meets their needs without compromising individuals' right to adequate notice of covered entities' information practices.

We note that covered entities may also be subject to the Electronic Signatures in Global and National Commerce Act. This rule is not intended to alter covered entities' requirements under that Act.

Comment: Some commenters were concerned that covered providers with ''face-to-face'' patient contact would have a competitive disadvantage against covered internet-based providers, because the face-to-face providers would be required to distribute the notice in hard copy while internet-based providers could satisfy the requirement

by requiring review of the notice on the web site before processing an order. They suggested allowing face-to-face covered providers to satisfy the distribution requirement by asking patients to review the notice posted on site.

Response: We clarify in the final rule that covered health care providers that provide services to individuals over the internet have direct treatment relationships with those individuals. Covered internet-based providers, therefore, must distribute the notice at the first service delivery after the compliance date by automatically and contemporaneously providing the notice electronically in response to the individual's first request for service, provided the individual agrees to receiving the notice electronically.

Even though we require all covered entity web sites to post the entity's notice prominently, we note that such posting is not sufficient to meet the distribution requirements. A covered internet-based provider must send the notice electronically at the individual's first request for service, just as other covered providers with direct treatment relationships must give individuals a copy of the notice as of the first service delivery after the compliance date.

We do not intend to create competitive advantages among covered providers. A web-based and a non-web-based covered provider each have the same alternatives available for distribution of the notice. Both types of covered providers may provide either a paper copy or an electronic copy of the notice.

Comment: We received several comments suggesting that some covered entities should be exempted from the notice requirement or permitted to combine notices with other covered entities. Many comments argued that the notice requirement would be burdensome for hospital-based physicians and result in numerous, duplicative notices that would be meaningless or confusing to patients. Other comments suggested that multiple health plans offered through the same employer should be permitted to produce a single notice.

Response: We retain the requirement for all covered health care providers and health plans to produce a notice of information practices. Health care clearinghouses are required to produce a notice of information practices only to the extent the clearinghouse creates or receives protected health information other than as a business associate of a covered entity. See § 164.500(b)(2). Two other types of covered entities are not required to produce a notice: a correctional institution that is a covered entity and a group health plan that provides benefits only through one or more contracts of insurance with health insurance issuers or HMOs.

We clarify in § 164.504(d), however, that affiliated covered entities under common ownership or control may designate themselves as a single covered entity for purposes of this rule. An affiliated covered entity is only required to produce a single notice.

In addition, covered entities that participate in an organized health care arrangement—which could include hospitals and their associated physicians—may choose to produce a single, joint notice, if certain requirements are met. See § 164.501 and the corresponding preamble discussion of organized health care arrangements.

We clarify that each covered entity included in a joint notice must meet the applicable distribution requirements. If any one of the covered entities, however, provides the notice to a given individual, the distribution requirement with respect to that individual is met for all of the covered entities included in the joint notice. For example, a covered hospital and its attending physicians may elect to produce a joint notice. When an individual is first seen at the hospital, the hospital must provide the individual with a copy of the joint notice. Once the hospital has done so, the notice distribution requirement for all of the attending physicians that provide treatment to the individual at the hospital and that are included in the joint notice is satisfied.

Comment: We solicited and received comments on whether to require covered entities to obtain the individual's signature on the notice. Some commenters suggested that requiring a signature would convey the importance of the notice, would make it more likely that individuals read the notice, and could have some of the same benefits of a consent. They noted that at least one state already requires entities to make a reasonable effort to obtain a signed notice. Other comments noted that the signature would be useful for compliance and risk management purposes because it would document that the individual had received the notice.

The majority of commenters on this topic, however, argued that a signed acknowledgment would be administratively burdensome, inconsistent with the intent of the Administrative Simplification requirements of HIPAA, impossible to achieve for incapacitated individuals, difficult to achieve for covered entities that do not have direct contact with patients, inconsistent with other notice requirements under other laws, misleading to individuals who might interpret their signature as an agreement, inimical to the concept of permitting uses and disclosures without authorization, and an insufficient substitute for authorization.

Response: We agree with the majority of commenters and do not require covered entities to obtain the individual's signed acknowledgment of receipt of the notice. We believe that we satisfied most of the arguments in support of requiring a signature with the new policy requiring covered health care providers with direct treatment relationships to obtain a consent for uses and disclosures of protected health information to carry out treatment, payment, and health care operations. See § 164.506 and the corresponding preamble discussion of consent requirements. We note that this rule does not preempt other applicable laws that require a signed notice and does not prohibit a covered entity from requesting an individual to sign the notice.

Comment: Some commenters supported requiring covered entities to adhere to their privacy practices, as described in their notice. They argued that the notice is meaningless if a covered entity does not actually have to follow the practices contained in its notice. Other commenters were concerned that the rule would prevent a covered entity from using or disclosing protected health information in otherwise lawful and legitimate ways because of an intentional or inadvertent omission from its published notice. Some of these commenters suggested requiring the notice to include a description of some or all disclosures that are required or permitted by law. Some commenters stated that the adherence requirement should be eliminated because it would generally inhibit covered entities' ability to innovate and would be burdensome.

Response: We agree that the value of the notice would be significantly diminished absent a requirement that covered entities adhere to the statements they make in their notices. We therefore retain the requirement for covered entities to adhere to the terms of the notice. See § 164.502(i).

Many of these commenters' concerns regarding a covered entity's inability to use or disclose protected health information due to an intentional or inadvertent omission from the notice are addressed in our revisions to the proposed content requirements for the notice. Rather than require covered entities to describe only those uses and

disclosures they anticipate making, as proposed, we require covered entities to describe all uses and disclosures they are required or permitted to make under the rule without the individual's consent or authorization. We permit a covered entity to provide a statement that it will disclose protected health information that is otherwise required by law, as permitted in § 164.512(a), without requiring them to list all state laws that may require disclosure. Because the notice must describe all legally permissible uses and disclosures, the notice will not generally preclude covered entities from making any uses or disclosures they could otherwise make without individual consent or authorization. This change will also ensure that individuals are aware of all possible uses and disclosures that may occur without their consent or authorization, regardless of the covered entity's current practices.

We encourage covered entities, however, to additionally describe the more limited uses and disclosures they actually anticipate making in order to give individuals a more accurate understanding of how information about them will be shared. We expect that certain covered entities will want to distinguish themselves on the basis of their privacy protections. We note that a covered entity that chooses to exercise this option must clearly state that, at a minimum, the covered entity may make disclosures that are required by law and that are necessary to avert a serious and imminent threat to health or safety.

Section 164.522—Rights To Request Privacy Protection for Protected Health Information

Section 164.522(a)—Right of an Individual To Request Restriction of Uses and Disclosures

Comment: Several commenters supported the language in the NPRM regarding the right to request restrictions. One commenter specifically stated that this is a balanced approach that addresses the needs of the few who would have reason to restrict disclosures without negatively affecting the majority of individuals. At least one commenter explained that if we required consent or authorization for use and disclosure of protected health information for treatment, payment, and health care operations then we must also have a right to request restrictions of such disclosure in order to make the consent meaningful.

Many commenters requested that we delete this provision, claiming it would interfere with patient care, payment, and data integrity. Most of the commenters that presented this position asserted that the framework of giving patients control over the use or disclosure of their information is contrary to good patient care because incomplete medical records may lead to medical errors, misdiagnoses, or inappropriate treatment decisions. Other commenters asserted that covered entities need complete data sets on the populations they serve to effectively conduct research and quality improvement projects and that restrictions would hinder research, skew findings, impede quality improvement, and compromise accreditation and performance measurement.

Response: We acknowledge that widespread restrictions on the use and disclosure of protected health information could result in some difficulties related to payment, research, quality assurance, etc. However, in our efforts to protect the privacy of health information about individuals, we have sought a balance in determining the appropriate level of individual control and the smooth operation of the health care system. In the final rule, we require certain covered providers and permit all covered entities to obtain consent from individuals for use and disclosure of protected health information for treatment, payment, and health care operations (see § 164.506). In order to give individuals some control over their health information for uses and disclosures of protected health information for treatment, payment, and health care operations, we provide individuals with the opportunity to request restrictions of such uses and disclosures.

Because the right to request restrictions encourages discussions about how protected health information may be used and disclosed and about an individual's concerns about such uses and disclosures, it may improve communications between a provider and patient and thereby improve care. According to a 1999 survey on the Confidentiality of Medical Records by the California HealthCare Foundation, one out of every six people engage in behavior to protect themselves from unwanted disclosures of health information, such as lying to providers or avoiding seeking care. This indicates that, without the ability to request restrictions, individuals would have incentives to remain silent about important health information that could have an effect on their health and health care, rather than consulting a health care provider.

Further, this policy is not a dramatic change from the status quo. Today, many state laws restrict disclosures for certain types of health information without patient's authorization. Even if there is no mandated requirement to restrict disclosures of health information, providers may agree to requests for restrictions of disclosures when a patient expresses particular sensitivity and concern for the disclosure of health information.

We agree that there may be instances in which a restriction could negatively affect patient care. Therefore, we include protections against this occurrence. First, the right to request restrictions is a right of individuals to make the request. A covered entity may refuse to restrict uses and disclosures or may agree only to certain aspects of the individual's request if there is concern for the quality of patient care in the future. For example, if a covered provider believes that it is not in the patient's best medical interest to have such a restriction, the provider may discuss the request for restriction with the patient and give the patient the opportunity to explain the concern for disclosure. Also, a covered provider who is concerned about the implications on future treatment can agree to use and disclose sensitive protected health information for treatment purposes only and agree not to disclose information for payment and operation purposes. Second, a covered provider need not comply with a restriction that has been agreed to if the individual who requested the restriction is in need of emergency treatment and the restricted protected health information is needed to provide the emergency treatment. This exception should limit the harm to health that may otherwise result from restricting the use or disclosure of protected health information. We encourage covered providers to discuss with individuals that the information may be used or disclosed in emergencies. We require that the covered entity that discloses restricted protected health information in an emergency request that the health care provider that receives such information not further use or re-disclose the information.

Comment: Some health plans stated that an institutionalized right to restrict can interfere with proper payment and can make it easier for unscrupulous providers or patients to commit fraud on insurance plans. They were concerned that individuals could enter into restrictions with providers to withhold information to insurance companies so that the insurance company would not know about certain conditions when underwriting a policy.

Response: This rule does not enhance the ability of unscrupulous patients or health care providers to engage in deceptive or fraudulent withholding of information. This rule grants a right to request a restriction, not an absolute right to restrict. Individuals can make such requests today. Other laws criminalize insurance fraud; this regulation does not change those laws.

Comment: One commenter asserted that patients cannot anticipate the significance that one aspect of their medical information will have on treatment of other medical conditions, and therefore, allowing them to restrict use or disclosure of some information is contrary to the patient's best interest.

Response: We agree that patients may find it difficult to make such a calculus, and that it is incumbent on health care providers to help them do so. Health care providers may deny requests for or limit the scope of the restriction requested if they believe the restriction is not in the patient's best interest.

Comment: One commenter asked whether an individual's restriction to disclosure of information will be a bar to liability for misdiagnosis or failure to diagnose by a covered entity who can trace its error back to the lack of information resulting from such restriction.

Response: Decisions regarding liability and professional standards are determined by state and other law. This rule does not establish or limit liability for covered entities under those laws. We expect that the individual's request to restrict the disclosure of their protected health information would be considered in the decision of whether or not a covered entity is liable.

Comment: One commenter requested that we allow health plans to deny coverage or reimbursement when a covered health care provider's agreement to restrict use or disclosure prevents the plan from getting the information that is necessary to determine eligibility or coverage.

Response: In this rule, we do not modify insurers' rules regarding information necessary for payment. We recognize that restricting the disclosure of information may result in a denial of payment. We expect covered providers to explain this possibility to individuals when considering their requests for restrictions and to make alternative payment arrangements with individuals if necessary.

Comment: Some commenters discussed the administrative burden and cost of the requirement that individuals have the right to request restrictions and that trying to segregate certain portions of information for protection may be impossible. Others stated that the administrative burden would make providers unable to accommodate restrictions, and would therefore give patients false expectations that their right to request restrictions may be acted upon. One commenter expressed concern that large covered providers would have a particularly difficult time establishing a policy whereby the covered entity could agree to restrictions and would have an even more difficult time implementing the restrictions since records may be kept in multiple locations and accessed by multiple people within the organization. Still other commenters believed that the right to request restrictions would invite argument, delay, and litigation.

Response: We do not believe that this requirement is a significant change from current practice. Providers already respond to requests by patients regarding sensitive information, and are subject to state law requirements not to disclose certain types of information without authorization. This right to request is permissive so that covered entities can balance the needs of particular individuals with the entity's ability to manage specific accommodations.

Comment: Some commenters were concerned that a covered entity would agree to a restriction and then realize later that the information must be disclosed to another caregiver for important medical care purposes.

Response: Some individuals seek treatment only on the condition that information about that treatment will not be shared with others. We believe it is necessary and appropriate, therefore, that when a covered provider agrees to such a restriction, the individual must be able to rely on that promise. We strongly encourage covered providers to consider future treatment implications of agreeing to a restriction. We encourage covered entities to inform others of the existence of a restriction when appropriate, provided that such notice does not amount to a *de facto* disclosure of the restricted information. If the covered provider subject to the restriction believes that disclosing the protected health information that was created or obtained subject to the restriction is necessary to avert harm (and it is not for emergency treatment), the provider must ask the individual for permission to terminate or modify the restriction. If the individual agrees to the termination of the restriction, the provider must document this termination by noting this agreement in the medical record or by obtaining a written agreement of termination from the individual and may use or disclose the information for treatment. If the individual does not agree to terminate or modify the restriction, however, the provider must continue to honor the restriction with respect to protected health information that was created or received subject to the restriction. We note that if the restricted protected health information is needed to provide emergency treatment to the individual who requested the restriction, the covered entity may use or disclose such information for such treatment.

Comment: Commenters asked that we require covered entities to keep an accounting of the requests for restrictions and to report this information to the Department in order for the Department to determine whether covered entities are showing ''good faith'' in dealing with these requests.

Response: We require that covered entities that agree to restrictions with individuals document such restrictions. A covered entity must retain such documentation for six years from the date of its creation or the date when it last was in effect, whichever is later. We do not require covered entities to keep a record of all requests made, including those not agreed to, nor that they report such requests to the Department. The decision to agree to restrictions is that of the covered entity. Because there is no requirement to agree to a restriction, there is no reason to impose the burden to document requests that are denied. Any reporting requirement could undermine the purpose of this provision by causing the sharing, or appearance of sharing, of information for which individuals are seeking extra protection.

Comment: One commenter asserted that providers that currently allow such restrictions will choose not to do so under the rule based on the guidance of legal counsel and loss prevention managers, and suggested that the Secretary promote competition among providers with respect to privacy by developing a third-party ranking mechanism.

Response: We believe that providers will do what is best for their patients, in accordance with their ethics codes, and will continue to find ways to accommodate requested restrictions when they believe that it is in the patients' best interests. We anticipate that providers who find such action to be of commercial benefit will notify consumers of their willingness to be responsive to such requests. Involving third parties could undermine the purpose of this provision, by causing the sharing, or appearance of sharing, of information for which individuals are seeking extra protection.

Comment: One commenter said that any agreement regarding patient-requested restrictions should be in writing before a covered provider would be held to standards for compliance.

Response: We agree that agreed to restrictions must be documented in writing, and we require that covered entities that agree to restrictions document those restrictions in accordance with § 164.530(j). The writing need not be formal; a notation in the medical record will suffice. We disagree with the request that an agreed to restriction be reduced to writing in order to be enforced. If we adopted the requested policy, a covered entity could agree to a restriction with an individual, but avoid being held to this agreed to restriction under the rule by failing to document the restriction. This would give a covered entity the opportunity to agree to a restriction and then, at its sole discretion, determine if it is enforceable by deciding whether or not to make a note of the restriction in the record about the individual. Because the covered entity has the ability to agree or fail to agree to a restriction, we believe that once the restriction is agreed to, the covered entity must honor the agreement. Any other result would be deceptive to the individual and could lead an individual to disclose health information under the assumption that the uses and disclosures will be restricted. Under § 164.522, a covered entity could be found to be in violation of the rule if it fails to put an agreed-upon restriction in writing and also if it uses or discloses protected health information inconsistent with the restriction.

Comment: Some commenters said that the right to request restrictions should be extended to some of the uses and disclosures permitted without authorization in § 164.510 of the NPRM, such as disclosures to next of kin, for judicial and administrative proceedings, for law enforcement, and for governmental health data systems. Other commenters said that these uses and disclosures should be preserved without an opportunity for individuals to opt out.

Response: We have not extended the right to request restrictions under this rule to disclosures permitted in § 164.512 of the final rule. However, we do not preempt other law that would enforce such agreed-upon restrictions. As discussed in more detail, above, we have extended the right to request restrictions to disclosures to persons assisting in the individual's care, such as next of kin, under § 164.510(b). Any restriction that a covered entity agrees to with respect to persons assisting in the individual's care in accordance with the rule will be enforceable under the rule.

Comment: A few commenters raised the question of the effect of a restriction agreed to by one covered entity that is part of a larger covered entity, particularly a hospital. Commenters were also concerned about who may speak on behalf of the covered entity.

Response: All covered entities are required to establish policies and procedures for providing individuals the right to request restrictions, including policies for who may agree to such restrictions on the covered entity's behalf. Hospitals and other large entities that are concerned about employees agreeing to restrictions on behalf of the organization will have to make sure that their policies are communicated appropriately to those employees. The circumstances under which members of a covered entity's workforce can bind the covered entity are a function of other law, not of this regulation.

Comment: Commenters expressed confusion about the intended effect of any agreed-upon restrictions on downstream covered entities. They asserted that it would be extremely difficult for a requested restriction to be followed through the health care system and that it would be unfair to hold covered entities to a restriction when they did not agree to such restriction. Specifically, commenters asked whether a covered provider that receives protected health information in compliance with this rule from a physician or medical group that has agreed to limit certain uses of the information must comply with the original restriction. Other commenters expressed concern that not applying a restriction to downstream covered entities is a loophole and that all downstream covered providers and health plans should be bound by the restrictions.

Response: Under the final rule, a restriction that is agreed to between an individual and a covered entity is only binding on the covered entity that agreed to the restriction and not on downstream entities. It would also be binding on any business associate of the covered entity since a business associate can not use or disclose protected health information in any manner that a covered entity would not be permitted to use or disclose such information. We realize that this may limit the ability of an individual to successfully restrict a use or disclosure under all circumstances, but we take this approach for two reasons. First, we allow covered entities to refuse individuals' requests for restrictions. Requiring downstream covered entities to abide by a restriction would be tantamount to forcing them to agree to a request to which they otherwise may not have agreed. Second, some covered entities have information systems which will allow them to accommodate such requests, while others do not. If the downstream provider is in the latter category, the administrative burden of such a requirement would be unmanageable.

We encourage covered entities to explain this limitation to individuals when they agree to restrictions, so individuals will understand that they need to ask all their health plans and providers for desired restrictions. We also require that a covered entity that discloses protected health information to a health care provider for emergency treatment, in accordance with § 164.522 (a)(iii), to request that the recipient not further use or disclose the information.

Comment: One commenter requested that agreed-to restrictions of a covered entity not be applied to business associates.

Response: As stated in § 164.504(e)(2), business associates are acting on behalf of, or performing services for, the covered entity and may not, with two narrow exceptions, use or disclose protected health information in a manner that would violate this rule if done by the covered entity. Business associates are agents of the covered entity with respect to protected health information they obtain through the business relationship. If the covered entity agrees to a restriction and, therefore, is bound to such restriction, the business associate will also be required to comply with the restriction. If the covered entity has agreed to a restriction, the satisfactory assurances from the business associate, as required in § 164.504(e), must include assurances that protected health information will not be used or disclosed in violation of an agreed to restriction.

Comment: One commenter requested clarification that the right to request restrictions cannot be used to restrict the creation of de-identified information.

Response: We found no reason to treat the use of protected health information to create de-identified information different from other uses of protected health information. The right to request restriction applies to any use or disclosure of protected health information to carry out treatment, payment, or health care operations. If the covered entity uses protected health information to create de-identified information, the covered entity need not agree to a restriction of this use.

Comment: Some commenters stated that individuals should be given a true right to restrict uses and disclosures of protected health information in certain defined circumstances (such as for sensitive information) rather than a right to request restrictions.

Response: We are concerned that a right to restrict could create conflicts with the professional ethical obligations of providers and others. We believe it is better policy to allow covered entities to refuse to honor restrictions that they believe are not appropriate and leave the individual with the option of seeking service from a different covered entity. In addition, many covered entities have information systems that would make it difficult or impossible to accommodate certain restrictions.

Comment: Some commenters requested that self-pay patients have additional rights to restrict protected health information. Others believed that this policy would result in de facto discrimination against those patients that could not afford to pay out-of-pocket.

Response: Under the final rule, the decision whether to tie an agreement to restrict to the way the individual pays for services is left to each covered entity. We have not provided self-pay patients with any special rights under the rule.

Comment: Some commenters suggested that we require restrictions to be clearly noted so that insurers and other providers would be aware that they were not being provided with complete information.

Response: Under the final rule, we do not require or prohibit a covered entity to note the existence of an omission of information. We encourage covered entities to inform others of the existence of a restriction, in accordance with professional practice and ethics, when appropriate to do so. In deciding whether or not to disclose the existence of a restriction, we encourage the covered entity to carefully consider whether disclosing the existence is tantamount to disclosure of the restricted protected health information so as to not violate the agreed to restriction.

Comment: A few commenters said that covered entities should have the right to modify or revoke an agreement to restrict use or disclosure of protected health information.

Response: We agree that, as circumstances change, covered entities should be able to revisit restrictions to which they had previously agreed. At the same time, individuals should be able to rely on agreements to restrict the use or disclosure of information that they believe is particularly sensitive. If a covered entity would like to revoke or modify an agreed-upon restriction, the covered entity must renegotiate the agreement with the individual. If the individual agrees to modify or terminate the restriction, the covered entity must get written agreement from the individual or must document the oral agreement. If the individual does not agree to terminate or modify the restriction, the covered entity must inform the individual that it is modifying or terminating its agreement to the restriction and any modification or termination would apply only with respect to protected health information created or received after the covered entity informed the individual of the termination. Any protected health information created or received during the time between when the restriction was agreed to and when the covered entity informed the individual or such modification or termination remains subject to the restriction.

Comment: Many commenters advocated for stronger rights to request restrictions, particularly that victims of domestic violence should have an absolute right to restrict disclosure of information.

Response: We address restrictions for disclosures in two different ways, the right to request restrictions (§ 164.522(a)) and confidential communications (§ 164.522(b)). We have provided all individuals with a right to request restrictions on uses or disclosures of treatment, payment, and health care operations. This is not an absolute right to restrict. Covered entities are not required to agree to requested restrictions; however, if they do, the rule would require them to act in accordance with the restrictions. (See the preamble regarding § 164.522 for a more comprehensive discussion of the right to request restrictions.)

In the final rule, we create a new provision that provides individuals with a right to confidential communications, in response to these comments. This provision grants individuals with a right to restrict disclosures of information related to communications made by a covered entity to the individual, by allowing the individual to request that such communications be made to the person at an alternative location or by an alternative means. For example, a woman who lives with an abusive man and is concerned that his knowledge of her health care treatment may lead to additional abuse can request that any mail from the provider be sent to a friend's home or that telephone calls by a covered provider be made to her at work. Other reasonable accommodations may be requested as well, such as requesting that a covered provider never contact the individual by a phone, but only contact her by electronic mail. A provider must accommodate an individual's request for confidential communications, under this section, without requiring an explanation as to the reason for the request as a condition of accommodating the request. The individual does not need to be in an abusive situation to make such requests of a covered provider. The only conditions that a covered provider may place on an individual is that the request be reasonable with respect to the administrative burden on the provider, the request to be in writing, the request specify an alternative address or other method of contact, and that (where relevant) the individual provide information about how payment will be handled. What is reasonable may vary by the size or type of covered entity; however, additional modest cost to the provider would not be unreasonable.

An individual also has a right to restrict communications from a health plan. The right is the same as with covered providers except it is limited to cases where the disclosure of information could endanger the individual. A health plan may require an individual to state this fact as a condition of accommodating the individual's request for confidential communications. This would provide victims of domestic violence the right to control such disclosures.

Comment: Commenters opposed the provision of the NPRM (§ 164.506(c)(1)(ii)(B)) stating that an individual's right to request restrictions on use or disclosure of protected health information would not apply in emergency situations as set forth in proposed § 164.510(k). Commenters asserted that victims who have been harmed by violence may first turn to emergency services for help and that, in such situations, the victim should be able to request that the perpetrator not be told of his or her condition or whereabouts.

Response: We agree with some of the commenters' concerns. In the final rule, the right to request restrictions is available to all individuals regardless of the circumstance or the setting in which the individual is obtaining care. For example, an individual that seeks care in an emergency room has the same right to request a restriction as an individual seeking care in the office of a covered physician.

However, we continue to permit a covered entity to disclose protected health information to a health care

provider in an emergency treatment situation if the restricted protected health information is needed to provide the emergency treatment or if the disclosure is necessary to avoid serious and imminent threats to public health and safety. Although we understand the concern of the commenters, we believe that these exceptions are limited and will not cause a covered entity to disclose information to a perpetrator of a crime. We are concerned that a covered provider would be required to delay necessary care if a covered entity had to determine if a restriction exists at the time of such emergency. Even if a covered entity knew that there was a restriction, we permitted this limited exception for emergency situations because, as we had stated in the preamble for § 164.506 of the NPRM, an emergency situation may not provide sufficient opportunity for a patient and health care provider to discuss the potential implications of restricting use and disclosure of protected health information on that emergency. We also believe that the importance of avoiding serious and imminent threats to health and safety and the ethical and legal obligations of covered health care providers' to make disclosures for these purposes is so significant that it is not appropriate to apply the right to request restrictions on such disclosures.

We note that we have included other provisions in the final rule intended to avoid or minimize harm to victims of domestic violence. Specifically, we include provisions in the final rule that allow individuals to opt out of certain types of disclosures and require covered entities to use professional judgment to determine whether disclosure of protected health information is in a patient's best interest (see § 164.510(a) on use and disclosure for facility directories and § 164.510(b) on uses and disclosures for assisting in an individual's care and notification purposes). Although an agreed to restriction under § 164.522 would apply to uses and disclosures for assisting in an individual's care, the opt out provision in § 164.510(b) can be more helpful to a person who is a victim of domestic violence because the individual can opt out of such disclosure without obtaining the agreement of the covered provider. We permit a covered entity to elect not to treat a person as a personal representative (see § 164.502(g)) or to deny access to a personal representative (see § 164.524(a)(3)(iii)) where there are concerns related to abuse. We also include a new § 164.512(c) which recognizes the unique circumstances surrounding disclosure of protected health information about victims of abuse, neglect, and domestic violence.

Section 164.522(b)—Confidential Communications Requirements

Comment: Several commenters requested that we add a new section to prevent disclosure of sensitive health care services to members of the patient's family through communications to the individual's home, such as appointment notices, confirmation or scheduling of appointments, or mailing a bill or explanation of benefits, by requiring covered entities to agree to correspond with the patient in another way. Some commenters stated that this is necessary in order to protect inadvertent disclosure of sensitive information and to protect victims of domestic violence from disclosure to an abuser. A few commenters suggested that a covered entity should be required to obtain an individual's authorization prior to communicating with the individual at the individual's home with respect to health care relating to sensitive subjects such as reproductive health, sexually transmissible diseases, substance abuse or mental health.

Response: We agree with commenters' concerns regarding covered entities' communications with individuals. We created a new provision, § 164.522(b), to address confidential communications by covered entities. This provision gives individuals the right to request that they receive communications from covered entities at an alternative address or by an alternative means, regardless of the nature of the protected health information involved. Covered providers are required to accommodate reasonable requests by individuals and may not require the individual to explain the basis for the request as a condition of accommodation. Health plans are required to accommodate reasonable requests by individuals as well; however, they may require the individual to provide a statement that disclosure of the information could endanger the individual, and they may condition the accommodation on the receipt of such statement.

Under the rule, we have required covered providers to accommodate requests for communications to alternative addresses or by alternative means, regardless of the reason, to limit risk of harm. Providers have more frequent one-on-one communications with patients, making the safety concerns from an inadvertent disclosure more substantial and the need for confidential communications more compelling. We have made the requirement for covered providers absolute and not contingent on the reason for the request because we wanted to make it relatively easy for victims of domestic violence, who face real safety concerns by disclosures of health information, to limit the potential for such disclosures.

The standard we created for health plans is different from the requirement for covered providers, in that we only require health plans to make requested accommodations for confidential communications when the individual asserts that disclosure could be dangerous to the individual. We address health plan requirements in this way because health plans are often issued to a family member (the employee), rather than to each individual member of a family, and therefore, health plans tend to communicate with the named insured rather than with individual family members. Requiring plans to accommodate a restriction for one individual could be administratively more difficult than it is for providers that regularly communicate with individuals. However, in the case of domestic violence or potential abuse, the level of harm that can result from a disclosure of protected health information tips the balance in favor of requiring such restriction to prevent inadvertent disclosure. We have adopted the policy recommended by the National Association of Insurance Commissioners in the Health Information Policy Model Act (1998) as this best reflects the balance of the appropriate level of regulation of the industry compared with the need to protect individuals from harm that may result from inadvertent disclosure of information. This policy is also consistent with recommendations made in the Family Violence Prevention Fund's publication ''Health Privacy Principles for Protecting Victims of Domestic Violence'' (October 2000). Of course, health plans may accommodate requests for confidential communications without requiring a statement that the individual would be in danger from disclosure of protected health information.

Comment: One commenter requested that we create a standard that all information from a health plan be sent to the patient and not the policyholder or subscriber.

Response: We require health plans to accommodate certain requests that information not be sent to a particular location or by particular means. A health plan must accommodate reasonable requests by individuals that protected health information about them be sent directly to them and not to a policyholder or subscriber, if the

individual states that he or she may be in danger from disclosure of such information. We did not generally require health plans to send information to the patient and not the policyholder or subscriber because we believed it would be administratively burdensome and because the named insured may have a valid need for such information to manage payment and benefits.

Sensitive Subjects

Comment: Many commenters requested that additional protections be placed on sensitive information, including information regarding HIV/AIDS, sexually transmitted diseases, mental health, substance abuse, reproductive health, and genetics. Many requested that we ensure the regulation adequately protects victims of domestic violence. They asserted that the concern for discrimination or stigma resulting from disclosure of sensitive health information could dissuade a person from seeking needed treatment. Some commenters noted that many state laws provide additional protections for various types of information. They requested that we develop federal standards to have consistent rules regarding the protection of sensitive information to achieve the goals of cost savings and patient protection. Others requested that we require patient consent or special authorization before certain types of sensitive information was disclosed, even for treatment, payment, and health care operations, and some thought we should require a separate request for each disclosure. Some commenters requested that the right to request restrictions be replaced with a requirement for an authorization for specific types of sensitive information. There were recommendations that we require covered entities to develop internal policies to address sensitive information.

Other commenters argued that sensitive information should not be segregated from the record because it may limit a future provider's access to information necessary for treatment of the individual and it could further stigmatize a patient by labeling him or her as someone with sensitive health care issues. These commenters further maintained that segregation of particular types of information could negatively affect analysis of community needs, research, and would lead to higher costs of health care delivery.

Response: We generally do not differentiate among types of protected health information, because all health information is sensitive. The level of sensitivity varies not only with the type of information, but also with the individual and the particular situation faced by the individual. This is demonstrated by the different types of information that commenters singled out as meriting special protection, and in the great variation among state laws in defining and protecting sensitive information. Most states have a law providing heightened protection for some type of health information. However, even though most states have considered the issue of sensitive information, the variation among states in the type of information that is specially protected and the requirements for permissible disclosure of such information demonstrates that there is no national consensus.

Where, as in this case, most states have acted and there is no predominant rule that emerges from the state experience with this issue, we have decided to let state law predominate. The final rule only provides a floor of protection for health information and does not preempt state laws that provide greater protection than the rule. Where states have decided to treat certain information as more sensitive than other information, we do not preempt those laws.

To address the variation in the sensitivity of protected health information without defining specially sensitive information, we incorporate opportunities for individuals and covered entities to address specific sensitivities and concerns about uses and disclosures of certain protected health information that the patient and provider believe are particularly sensitive, as follows:

- Covered entities are required to provide individuals with notice of their privacy practices and give individuals the opportunity to request restrictions of the use and disclosure of protected health information by the covered entity. (See § 164.522(a) regarding right to request restrictions.)
- Individuals have the right to request, and in some cases require, that communications from the covered entity to them be made to an alternative address or by an alternative means than the covered entity would otherwise use. (See § 164.522(b) regarding confidential communications.)
- Covered entities have the opportunity to decide not to treat a person as a personal representative when the covered entity has a reasonable belief that an individual has been subjected to domestic violence, abuse, or neglect by such person or that treating such person as a personal representative could endanger the individual. (See § 164.502(g)(5) regarding personal representatives.)
- Covered entities may deny access to protected health information when there are concerns that the access may result in varying levels of harm. (See § 164.524(a)(3) regarding denial of access.)
- Covered health care providers may, in some circumstances and consistent with any known prior preferences of the individual, exercise professional judgment in the individual's best interest to not disclose directory information. (See § 164.510(a) regarding directory information.)
- Covered entities may, in some circumstances, exercise professional judgment in the individual's best interest to limit disclosure to persons assisting in the individual's care. (See § 164.510(b) regarding persons assisting in the individual's care.)

This approach allows for state law and personal variation in this area.

The only type of protected health information that we treat with heightened protection is psychotherapy notes. We provide a different level of protection because they are unique types of protected health information that typically are not used or required for treatment, payment, or health care operations other than by the mental health professional that created the notes. (See § 164.508(a)(2) regarding psychotherapy notes.)

Section 164.524—Access of Individuals to Protected Health Information

Comment: Some commenters recommended that there be no access to disease registries.

Response: Most entities that maintain disease registries are not covered entities under this regulation; examples of such non-covered entities are public health agencies and pharmaceutical companies. If, however, a disease registry is maintained by a covered entity and is used to make decisions about individuals, this rule requires the covered entity to provide access to information about a requesting individual unless one of the rule's conditions for denial of access is met. We found no persuasive reasons why disease registries should be given special treatment compared with other information that may be used to make decisions about an individual.

Comment: Some commenters stated that covered entities should be held accountable for access to information held by business partners so that individuals would not have the burden of tracking down their protected health information from a business partner. Many commenters, including insurers

and academic medical centers, recommended that, to reduce burden and duplication, only the provider who created the protected health information should be required to provide individuals access to the information. Commenters also asked that other entities, including business associates, the Medicare program, and pharmacy benefit managers, not be required to provide access, in part because they do not know what information the covered entity already has and they may not have all the information requested. A few commenters also argued that billing companies should not have to provide access because they have a fiduciary responsibility to their physician clients to maintain the confidentiality of records.

Response: A general principle in responding to all of these points is that a covered entity is required to provide access to protected health information in accordance with the rule regardless of whether the covered entity created such information or not. Thus, we agree with the first point: in order to meet its requirements for providing access, a covered entity must not only provide access to such protected health information it holds, but must also provide access to such information in a designated record set of its business associate, pursuant to its business associate contract, unless the information is the same as information maintained directly by the covered entity. We require this because an individual may not be aware of business associate relationships. Requiring an individual to track down protected health information held by a business associate would significantly limit access. In addition, we do not permit a covered entity to limit its duty to provide access by giving protected health information to a business associate.

We disagree with the second point: if the individual directs an access request to a covered entity that has the protected health information requested, the covered entity must provide access (unless it may deny access in accordance with this rule). In order to assure that an individual can exercise his or her access rights, we do not require the individual to make a separate request to each originating provider. The originating provider may no longer be in business or may no longer have the information, or the non-originating provider may have the information in a modified or enhanced form.

We disagree with the third point: other entities must provide access only if they are covered entities or business associates of covered entities, and they must provide access only to protected health information that they maintain (or that their business associates maintain). It would not be efficient to require a covered entity to compare another entity's information with that of the entity to which the request was addressed. (See the discussion regarding covered entities for information about whether a pharmacy benefit manager is a covered entity.)

We disagree with the fourth point: a billing company will be required by its business associate contract only to provide the requested protected health information to its physician client. This action will not violate any fiduciary responsibility. The physician client would in turn be required by the rule to provide access to the individual.

Comment: Some commenters asked for clarification that the clearinghouse function of turning non-standardized data into standardized data does not create non-duplicative data and that ''duplicate'' does not mean ''identical.'' A few commenters suggested that duplicated information in a covered entity's designated record set be supplied only once per request.

Response: We consider as duplicative information the same information in different formats, media, or presentations, or which have been standardized. Business associates who have materially altered protected health information are obligated to provide individuals access to it. Summary information and reports, including those of lab results, are not the same as the underlying information on which the summaries or reports were based. A clean document is not a duplicate of the same document with notations. If the same information is kept in more than one location, the covered entity has to produce the information only once per request for access.

Comment: A few commenters suggested requiring covered entities to disclose to third parties without exception at the requests of individuals. It was argued that this would facilitate disability determinations when third parties need information to evaluate individuals' entitlement to benefits. Commenters argued that since covered entities may deny access to individuals under certain circumstances, individuals must have another method of providing third parties with their protected health information.

Response: We allow covered entities to forward protected health information about an individual to a third party, pursuant to the individual's authorization under § 164.508. We do not require covered entities to disclose information pursuant to such authorizations because the focus of the rule is privacy of protected health information. Requiring disclosures in all circumstances would be counter to this goal. In addition, a requirement of disclosing protected health information to a third party is not a necessary substitute for the right of access to individuals, because we allow denial of access to individuals under rare circumstances. However, if the third party is a personal representative of the individual in accordance with § 164.502(g) and there is no concern regarding abuse or harm to the individual or another person, we require the covered entity to provide access to that third party on the individual's behalf, subject to specific limitations. We note that a personal representative may obtain access on the individual's behalf in some cases where covered entity may deny access to the individual. For example, an inmate may be denied a copy of protected health information, but a personal representative may be able to obtain a copy on the individual's behalf. See § 164.502(g) and the corresponding preamble discussion regarding the ability of a personal representative to act on an individual's behalf.

Comment: The majority of commenters supported granting individuals the right to access protected health information for as long as the covered entity maintains the protected health information; commenters argued that to do otherwise would interfere with existing record retention laws. Some commenters advocated for limiting the right to information that is less than one or two years old. A few commenters explained that frequent changes in technology makes it more difficult to access stored data. The commenters noted that the information obtained prior to the effective date of the rule should not be required to be accessible.

Response: We agree with the majority of commenters and retain the proposal to require covered entities to provide access for as long as the entity maintains the protected health information. We do not agree that information created prior to the effective date of the rule should not be accessible. The reasons for granting individuals access to information about them do not vary with the date the information was created.

Comment: A few commenters argued that there should be no grounds for denying access, stating that individuals should always have the right to inspect and copy their protected health information.

Response: While we agree that in the vast majority of instances individuals should have access to information about them, we cannot agree that a blanket rule would be appropriate. For example, where a professional familiar with the particular circumstances believes that providing such access is likely to endanger a person's life or physical safety, or where granting such access would violate the privacy of other individuals, the benefits of allowing access may not outweigh the harm. Similarly, we allow denial of access where disclosure would reveal the source of confidential information because we do not want to interfere with a covered entity's ability to maintain implicit or explicit promises of confidence.

We create narrow exceptions to the rule of open access, and we expect covered entities to employ these exceptions rarely, if at all. Moreover, we require covered entities to provide access to any protected health information requested after excluding only the information that is subject to a denial. The categories of permissible denials are not mandatory, but are a means of preserving the flexibility and judgment of covered entities under appropriate circumstances.

Comment: Many commenters supported our proposal to allow covered entities to deny an individual access to protected health information if a professional determines either that such access is likely to endanger the life or physical safety of a person or, if the information is about another person, access is reasonably likely to cause substantial harm to such person.

Some commenters requested that the rule also permit covered entities to deny a request if access might be reasonably likely to cause psychological or mental harm, or emotional distress. Other commenters, however, were particularly concerned about access to mental health information, stating that the lack of access creates resentment and distrust in patients.

Response: We disagree with the comments suggesting that we expand the grounds for denial of access to an individual to include a likelihood of psychological or mental harm of the individual. We did not find persuasive evidence that this is a problem sufficient to outweigh the reasons for providing open access. We do allow a denial for access based on a likelihood of substantial psychological or mental harm, but only if the protected health information includes information about another person and the harm may be inflicted on such other person or if the person requesting the access is a personal representative of the individual and the harm may be inflicted on the individual or another person.

We generally agree with the commenters concerns that denying access specifically to mental health records could create distrust. To balance this concern with other commenters' concerns about the potential for psychological harm, however, we exclude psychotherapy notes from the right of access. This is the only distinction we make between mental health information and other types of protected health information in the access provisions of this rule. Unlike other types of protected health information, these notes are not widely disseminated through the health care system. We believe that the individual's privacy interests in having access to these notes, therefore, are outweighed by the potential harm caused by such access. We encourage covered entities that maintain psychotherapy notes, however, to provide individuals access to these notes when they believe it is appropriate to do so.

Comment: Some commenters believed that there is a potential for abuse of the provision allowing denial of access because of likely harm to self. They questioned whether there is any experience from the Privacy Act of 1974 to suggest that patients who requested and received their records have ever endangered themselves as a result.

Response: We are unaware of such problems from access to records that have been provided under the Privacy Act but, since these are private matters, such problems might not come to our attention. We believe it is more prudent to preserve the flexibility and judgment of health care professionals familiar with the individuals and facts surrounding a request for records than to impose the blanket rule suggested by these commenters.

Comment: Commenters asserted that the NPRM did not adequately protect vulnerable individuals who depend on others to exercise their rights under the rule. They requested that the rule permit a covered entity to deny access when the information is requested by someone other than the subject of the information and, in the opinion of a licensed health care professional, access to the information could harm the individual or another person.

Response: We agree with the commenters that such protection is warranted and add a provision in § 164.524(a)(3), which permits a covered health care provider to deny access if a personal representative of the individual is making the request for access and a licensed health care professional has determined, in the exercise of professional judgment, that providing access to such personal representative could result in substantial harm to the individual or another person. Access can be denied even if the potential harm may be inflicted by someone other than the personal representative.

This provision is designed to strike a balance between the competing interests of ensuring access to protected health information and protecting the individual or others from harm. The ''substantial harm'' standard will ensure that a covered entity cannot deny access in cases where the harm is de minimus.

The amount of discretion that a covered entity has to deny access to a personal representative is generally greater than the amount of discretion that a covered entity has to deny access to an individual. Under the final rule, a covered entity may deny access to an individual if a licensed health care professional determines that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person. In this case, concerns about psychological or emotional harm would not be sufficient to justify denial of access. We establish a relatively high threshold because we want to assure that individuals have broad access to health information about them, and due to the potential harm that comes from denial of access, we believe denials should be permitted only in limited circumstances.

The final rule grants covered entities greater discretion to deny access to a personal representative than to an individual in order to provide protection to those vulnerable people who depend on others to exercise their rights under the rule and who may be subjected to abuse or neglect. This provision applies to personal representatives of minors as well as other individuals. The same standard for denial of access on the basis of potential harm that applies to personal representatives also applies when an individual is seeking access to his or her protected health information, and the information makes reference to another person. Under these circumstances, a covered entity may deny a request for access if such access is reasonably likely to cause substantial harm to such other person. The standard for this provision and for the provision regarding access by personal representatives is the same because both circumstances involve one person obtaining information about another person, and in both cases the covered entity is balancing the right of access of one person against the right of

a second person not to be harmed by the disclosure.

Under any of these grounds for denial of access to protected health information, the covered entity is not required to deny access to a personal representative under these circumstances, but has the discretion to do so.

In addition to denial of access rights, we also address the concerns raised by abusive or potentially abusive situations in the section regarding personal representatives by giving covered entities discretion to not recognize a person as a personal representative of an individual if the covered entity has a reasonable belief that the individual has been subjected to domestic violence, abuse, or neglect by or would be in danger from a person seeking to act as the personal representative. (See § 164.502(g))

Comment: A number of commenters were concerned that this provision would lead to liability for covered entities if the release of information results in harm to individuals. Commenters requested a ''good faith'' standard in this provision to relieve covered entities of liability if individuals suffer harm as a result of seeing their protected health information or if the information is found to be erroneous. A few commenters suggested requiring providers (when applicable) to include with any disclosure to a third party a statement that, in the provider's opinion, the information should not be disclosed to the patient.

Response: We do not intend to create a new duty to withhold information nor to affect other laws on this issue. Some state laws include policies similar to this rule, and we are not aware of liability arising as a result.

Comment: Some commenters suggested that both the individual's health care professional and a second professional in the relevant field of medicine should review each request. Many commenters suggested that individuals have a right to have an independent review of any denial of access, e.g., review by a health care professional of the individual's choice.

Response: We agree with the commenters who suggest that denial on grounds of harm to self or others should be determined by a health professional, and retain this requirement in the final rule. We disagree, however, that all denials should be reviewed by a professional of the individual's choice. We are concerned that the burden such a requirement would place on covered entities would be significantly greater than any benefits to the individual. We believe that any health professional, not just one of the individual's choice, will exercise appropriate professional judgment. To address some of these concerns, however, we add a provision for the review of denials requiring the exercise of professional judgment. If a covered entity denies access based on harm to self or others, the individual has the right to have the denial reviewed by another health care professional who did not participate in the original decision to deny access.

Comment: A few commenters objected to the proposal to allow covered entities to deny a request for access to health information if the information was obtained from a confidential source that may be revealed upon the individual's access. They argued that this could be subject to abuse and the information could be inherently less reliable, making the patient's access to it even more important.

Response: While we acknowledge that information provided by confidential sources could be inaccurate, we are concerned that allowing unfettered access to such information could undermine the trust between a health care provider and patients other than the individual. We retain the proposed policy because we do not want to interfere with a covered entity's ability to obtain important information that can assist in the provision of health care or to maintain implicit or explicit promises of confidence, which may be necessary to obtain such information. We believe the concerns raised about abuse are mitigated by the fact that the provision does not apply to promises of confidentiality made to a health care provider. We note that a covered entity may provide access to such information.

Comment: Some commenters were concerned that the NPRM did not allow access to information unrelated to treatment, and thus did not permit access to research information.

Response: In the final rule, we eliminate the proposed special provision for ''research information unrelated to treatment.'' The only restriction on access to research information in this rule applies where the individual agrees in advance to denial of access when consenting to participate in research that includes treatment. In this circumstance, the individual's right of access to protected health information created in the course of the research may be suspended for as long as the research is in progress, but access rights resume after such time. In other instances, we make no distinction between research information and other information in the access provisions in this rule.

Comment: A few commenters supported the proposed provision temporarily denying access to information obtained during a clinical trial if participants agreed to the denial of access when consenting to participate in the trial. Some commenters believed there should be no access to any research information. Other commenters believed denial should occur only if the trial would be compromised. Several recommended conditioning the provision. Some recommended that access expires upon completion of the trial unless there is a health risk. A few commenters suggested that access should be allowed only if it is included in the informed consent and that the informed consent should note that some information may not be released to the individual, particularly research information that has not yet been validated. Other commenters believed that there should be access if the research is not subject to IRB or privacy board review or if the information can be disclosed to third parties.

Response: We agree with the commenters that support temporary denial of access to information from research that includes treatment if the subject has agreed in advance, and with those who suggested that the denial of access expire upon completion of the research, and retain these provisions in the final rule. We disagree with the commenters who advocate for further denial of this information. These comments did not explain why an individual's interest in access to health information used to make decisions about them is less compelling with respect to research information. Under this rule, all protected health information for research is subject either to privacy board or IRB review unless a specific authorization to use protected health information for research is obtained from the individual. Thus, this is not a criterion we can use to determine access rights.

Comment: A few commenters believed that it would be ''extremely disruptive of and dangerous'' to patients to have access to records regarding their current care and that state law provides sufficient protection of patients' rights in this regard.

Response: We do not agree. Information about current care has immediate and direct impact on individuals. Where a health care professional familiar with the circumstances believes that it is reasonably likely that access to records would endanger the life or physical safety of the individual or another

person, the regulation allows the professional to withhold access.

Comment: Several commenters requested clarification that a patient not be denied access to protected health information because of failure to pay a bill. A few commenters requested clarification that entities may not deny requests simply because producing the information would be too burdensome.

Response: We agree with these comments, and confirm that neither failure to pay a bill nor burden are lawful reasons to deny access under this rule. Covered entities may deny access only for the reasons provided in the rule.

Comment: Some commenters requested that the final rule not include detailed procedural requirements about how to respond to requests for access. Others made specific recommendations on the procedures for providing access, including requiring written requests, requiring specific requests instead of blanket requests, and limiting the frequency of requests. Commenters generally argued against requiring covered entities to acknowledge requests, except under certain circumstances, because of the potential burden on entities.

Response: We intend to provide sufficient procedural guidelines to ensure that individuals have access to their protected health information, while maintaining the flexibility for covered entities to implement policies and procedures that are appropriate to their needs and capabilities. We believe that a limit on the frequency of requests individuals may make would arbitrarily infringe on the individual's right of access and have, therefore, not included such a limitation. To limit covered entities' burden, we do not require covered entities to acknowledge receipt of the individuals' requests, other than to notify the individual once a decision on the request has been made. We also permit a covered entity to require an individual to make a request for access in writing and to discuss a request with an individual to clarify which information the individual is actually requesting. If individuals agree, covered entities may provide access to a subset of information rather than all protected health information in a designated record set. We believe these changes provide covered entities with greater flexibility without compromising individuals' access rights.

Comment: Commenters offered varying suggestions for required response time, ranging from 48 hours because of the convenience of electronic records to 60 days because of the potential burden. Others argued against a finite time period, suggesting the response time be based on mutual convenience of covered entities and individuals, reasonableness, and exigencies. Commenters also varied on suggested extension periods, from one 30-day extension to three 30-day extensions to one 90-day extension, with special provisions for off-site records.

Response: We are imposing a time limit because individuals are entitled to know when to expect a response. Timely access to protected health information is important because such information may be necessary for the individual to obtain additional health care services, insurance coverage, or disability benefits, and the covered entity may be the only source for such information. To provide additional flexibility, we eliminate the requirement that access be provided as soon as possible and we lengthen the deadline for access to off-site records. For on-site records, covered entities must act on a request within 30 days of receipt of the request. For off-site records, entities must complete action within 60 days. We also permit covered entities to extend the deadline by up to 30 days if they are unable to complete action on the request within the standard deadline. These time limits are intended to be an outside deadline rather than an expectation. We expect covered entities to be attentive to the circumstances surrounding each request and respond in an appropriate time frame.

Comment: A few commenters suggested that, upon individuals' requests, covered entities should be required to provide protected health information in a format that would be understandable to a patient, including explanations of codes or abbreviations. The commenters suggested that covered entities be permitted to provide summaries of pertinent information instead of full copies of records; for example, a summary may be more helpful for the patient's purpose than a series of indecipherable billing codes.

Response: We agree with these commenters' point that some health information is difficult to interpret. We clarify, therefore, that the covered entity may provide summary information in lieu of the underlying records. A summary may only be provided if the covered entity and the individual agree, in advance, to the summary and to any fees imposed by the covered entity for providing such summary. We similarly permit a covered entity to provide an explanation of the information. If the covered entity charges a fee for providing an explanation, it must obtain the individual's agreement to the fee in advance.

Comment: Though there were recommendations that fees be limited to the costs of copying, the majority of commenters on this topic requested that covered entities be able to charge a reasonable, cost-based fee. Commenters suggested that calculation of access costs involve factors such as labor costs for verification of requests, labor and software costs for logging of requests, labor costs for retrieval, labor costs for copying, expense costs for copying, capital cost for copying, expense costs for mailing, postal costs for mailing, billing and bad-debt expenses, and labor costs for refiling. Several commenters recommended specific fee structures.

Response: We agree that covered entities should be able to recoup their reasonable costs for copying of protected health information, and include such provision in the regulation. We are not specifying a set fee because copying costs could vary significantly depending on the size of the covered entity and the form of such copy (*e.g.,* paper, electronic, film). Rather, covered entities are permitted to charge a reasonable, cost-based fee for copying (including the costs of supplies and labor), postage, and summary or explanation (if requested and agreed to by the individual) of information supplied. The rule limits the types of costs that may be imposed for providing access to protected health information, but does not preempt applicable state laws regarding specific allowable fees for such costs. The inclusion of a copying fee is not intended to impede the ability of individuals to copy their records.

Comment: Many commenters stated that if a covered entity denies a request for access because the entity does not hold the protected health information requested, the covered entity should provide, if known, the name and address of the entity that holds the information. Some of these commenters additionally noted that the Uniform Insurance Information and Patient Protection Act, adopted by 16 states, already imposes this notification requirement on insurance entities. Some commenters also suggested requiring providers who leave practice or move offices to inform individuals of that fact and of how to obtain their records.

Response: We agree that, when covered entities deny requests for access because they do not hold the protected health information requested, they should inform individuals of the holder of the information, if known; we include this provision in the final rule. We do not require health care providers to

notify all patients when they move or leave practice, because the volume of such notifications would be unduly burdensome.

Section 164.526—Amendment of Protected Health Information

Comment: Many commenters strongly encouraged the Secretary to adopt ''appendment'' rather than ''amendment and correction'' procedures. They argued that the term ''correction'' implies a deletion of information and that the proposed rule would have allowed covered entities to remove portions of the record at their discretion. Commenters indicated that appendment rather than correction procedures will ensure the integrity of the medical record and allow subsequent health care providers access to the original information as well as the appended information. They also indicated appendment procedures will protect both individuals and covered entities since medical records are sometimes needed for litigation or other legal proceedings.

Response: We agree with commenters' concerns about the term ''correction.'' We have revised the rule and deleted ''correction'' from this provision in order to clarify that covered entities are not required by this rule to delete any information from the designated record set. We do not intend to alter medical record retention laws or current practice, except to require covered entities to append information as requested to ensure that a record is accurate and complete. If a covered entity prefers to comply with this provision by deleting the erroneous information, and applicable record retention laws allow such deletion, the entity may do so. For example, an individual may inform the entity that someone else's X-rays are in the individual's medical record. If the entity agrees that the X-ray is inaccurately filed, the entity may choose to so indicate and note where in the record the correct X-ray can be found. Alternatively, the entity may choose to remove the X-ray from the record and replace it with the correct X-ray, if applicable law allows the entity to do so. We intend the term ''amendment'' to encompass either action.

We believe this approach is consistent with well-established privacy principles, with other law, and with industry standards and ethical guidelines. The July 1977 Report of the Privacy Protection Study Commission recommended that health care providers and other organizations that maintain medical-record information have procedures for individuals to correct or amend the information.[28] The Privacy Act (5 U.S.C. 552a) requires government agencies to permit individuals to request amendment of any record the individual believes is not accurate, relevant, timely, or complete. In its report ''Best Principles for Health Privacy,'' the Health Privacy Working Group recommended, ''An individual should have the right to supplement his or her own medical record. Supplementation should not be implied to mean deletion or alteration of the medical record.'' [29] The National Association of Insurance Commissioners' Health Information Privacy Model Act establishes the right of an individual who is the subject of protected health information to amend protected health information to correct any inaccuracies. The National Conference of Commissioners on Uniform State Laws' Uniform Health Care Information Act states, ''Because accurate health-care information is not only important to the delivery of health care, but for patient applications for life, disability and health insurance, employment, and a great many other issues that might be involved in civil litigation, this Act allows a patient to request an amendment in his record.''

Some states also establish a right for individuals to amend health information about them. For example, Hawaii law (HRS section 323C–12) states, ''An individual or the individual's authorized representative may request in writing that a health care provider that generated certain health care information append additional information to the record in order to improve the accuracy or completeness of the information; provided that appending this information does not erase or obliterate any of the original information.'' Montana law (MCA section 50–16–543) states, ''For purposes of accuracy or completeness, a patient may request in writing that a health care provider correct or amend its record of the patient's health care information to which he has access.'' Connecticut, Georgia, and Maine provide individuals a right to request correction, amendment, or deletion of recorded personal information about them maintained by an insurance institution. Many other states have similar provisions.

Industry and standard-setting organizations have also developed policies for amendment of health information. The National Committee for Quality Assurance and the Joint Commission on Accreditation of Healthcare Organizations issued recommendations stating, ''The opportunity for patients to review their records will enable them to correct any errors and may provide them with a better understanding of their health status and treatment. Amending records does not erase the original information. It inserts the correct information with a notation about the date the correct information was available and any explanation about the reason for the error.'' [30] Standards of the American Society for Testing and Materials state, ''An individual has a right to amend by adding information to his or her record or database to correct inaccurate information in his or her patient record and in secondary records and databases which contain patient identifiable health information.'' [31] We build on this well-established principle in this final rule.

Comment: Some commenters supported the proposal to allow individuals to request amendment for as long as the covered provider or plan maintains the information. A few argued that the provision should be time-limited, *e.g.,* that covered entities should not have to amend protected health information that is more than two years old. Other comments suggested that the provision should only be applied to protected health information created after the compliance date of the regulation.

Response: The purpose of this provision is to create a mechanism whereby individuals can ensure that information about them is as accurate as possible as it travels through the health care system and is used to make decisions, including treatment decisions, about them. To achieve this result, individuals must have the ability to request amendment for as long as the information used to make decisions about them exists. We therefore retain the proposed approach. For these reasons, we also require covered entities to address requests for amendment of all protected health information within designated record sets, including information created or obtained prior to

[28] Privacy Protection Study Commission, ''Personal Privacy in an Information Society,'' July 1977, p. 300–303.

[29] Health Privacy Working Group, ''Best Principles for Health Privacy,'' Health Privacy Project, Institute for Health Care Research and Policy, Georgetown University, July 1999.

[30] National Committee on Quality Assurance and the Joint Commission on Accreditation of Healthcare Organizations, ''Protecting Personal Health Information: A Framework for Meeting the Challenges in a Managed Care Environment,''1998, p. 25.

[31] ASTM, ''Standard Guide for Confidentiality, Privacy, Access and Data Security, Principles for Health Information Including Computer-Based Patient Records,'' E 1869–97, § 11.1.1.

the compliance date, for as long as the entity maintains the information.

Comment: A few commenters were concerned that the proposal implied that the individual is in control of and may personally change the medical record. These commenters opposed such an approach.

Response: We do not give individuals the right to alter their medical records. Individuals may request amendment, but they have no authority to determine the final outcome of the request and may not make actual changes to the medical record. The covered entity must review the individual's request and make appropriate decisions. We have clarified this intent in § 164.526(a)(1) by stating that individuals have a right to have a covered entity amend protected health information and in § 164.526(b)(2) by stating that covered entities must act on an individual's request for amendment.

Comment: Some comments argued that there is no free-text field in some current transaction formats that would accommodate the extra text required to comply with the amendment provisions (*e.g.,* sending statements of disagreement along with all future disclosures of the information at issue). Commenters argued that this provision will burden the efficient transmission of information, contrary to HIPAA requirements.

Response: We believe that most amendments can be incorporated into the standard transactions as corrections of erroneous data. We agree that some of the standard transactions cannot currently accommodate additional material such as statements of disagreement and rebuttals to such statements. To accommodate these rare situations, we modify the requirements in § 164.526(d)(iii). The provision now states that if a standard transaction does not permit the inclusion of the additional material required by this section, the covered entity may separately transmit the additional material to the recipient of the standard transaction. Commenters interested in modifying the standard transactions to allow the incorporation of additional materials may also bring the issue up for resolution through the process established by the Transactions Rule and described in its preamble.

Comment: The NPRM proposed to allow amendment of protected health information in designated record sets. Some commenters supported the concept of a designated record set and stated that it appropriately limits the type of information available for amendment to information directly related to treatment. Other commenters were concerned about the burden this provision will create due to the volume of information that will be available for amendment. They were primarily concerned with the potential for frivolous, minor, or technical requests. They argued that for purposes of amendment, this definition should be limited to information used to make medical or treatment decisions about the individual. A few commenters requested clarification that individuals do not have a right to seek amendment unless there is verifiable information to support their claim or they can otherwise convince the entity that the information is inaccurate or incomplete.

Response: We believe that the same information available for inspection should also be subject to requests for amendment, because the purpose of these provisions is the same: To give consumers access to and the chance to correct errors in information that may be used to make decisions that affect their interests. We thus retain use of the ''designated record set'' in this provision. However, we share commenters'' concerns about the potential for minor or technical requests. To address this concern, we have clarified that covered entities may deny a request for amendment if the request is not in writing and does not articulate a reason to support the request, as long as the covered entity informs the individual of these requirements in advance.

Comment: Many commenters noted the potentially negative impact of the proposal to allow covered entities to deny a request for amendment if the covered entity did not create the information at issue. Some commenters pointed out that the originator of the information may no longer exist or the individual may not know who created the information in question. Other commenters supported the proposal that only the originator of the information is responsible for amendments to it. They argued that any extension of this provision requiring covered entities to amend information they have not created is administratively and financially burdensome.

Response: In light of the comments, we modify the rule to require the holder of the information to consider a request for amendment if the individual requesting amendment provides a reasonable basis to believe that the originator of the information is no longer available to act on a request. For example, if a request indicates that the information at issue was created by a hospital that has closed, and the request is not denied on other grounds, then the entity must amend the information. This provision is necessary to preserve an individual's right to amend protected health information about them in certain circumstances.

Comment: Some commenters stated that the written contract between a covered entity and its business associate should stipulate that the business associate is required to amend protected health information in accordance with the amendment provisions. Otherwise, these commenters argued, there would be a gap in the individual's right to have erroneous information corrected, because the covered entity could deny a request for amendment of information created by a business associate.

Response: We agree that information created by the covered entity or by the covered entity's business associates should be subject to amendment. This requirement is consistent with the requirement to make information created by a business associate available for inspection and copying. We have revised the rule to require covered entities to specify in the business associate contract that the business associate will make protected health information available for amendment and will incorporate amendments accordingly. (See § 164.504(e).)

Comment: One commenter argued that covered entities should be required to presume information must be corrected where an individual informs the entity that an adjudicative process has made a finding of medical identity theft.

Response: Identity theft is one of many reasons why protected health information may be inaccurate, and is one of many subjects that may result in an adjudicative process relevant to the accuracy of protective health information. We believe that this provision accommodates this situation without a special provision for identity theft.

Comment: Some commenters asserted that the proposed rule's requirement that action must be taken on individuals' requests within 60 days of the receipt of the request was unreasonable and burdensome. A few commenters proposed up to three 30-day extensions for ''extraordinary'' (as defined by the entity) requests.

Response: We agree that 60 days will not always be a sufficient amount of time to adequately respond to these requests. Therefore, we have revised this provision to allow covered entities the option of a 30-day extension to deal with requests that require additional response time. However, we expect that 60 days will be adequate for most cases.

Comment: One commenter questioned whether a covered entity could

appropriately respond to a request by amending the record, without indicating whether it believes the information at issue is accurate and complete.

Response: An amendment need not include a statement by the covered entity as to whether the information is or is not accurate and complete. A covered entity may choose to amend a record even if it believes the information at issue is accurate and complete. If a request for amendment is accepted, the covered entity must notify the individual that the record has been amended. This notification need not include any explanation as to why the request was accepted. A notification of a denied request, however, must contain the basis for the denial.

Comment: A few commenters suggested that when an amendment is made, the date should be noted. Some also suggested that the physician should sign the notation.

Response: We believe such a requirement would create a burden that is not necessary to protect individuals' interests, and so have not accepted this suggestion. We believe that the requirements of § 164.526(c) regarding actions a covered entity must take when accepting a request will provide an adequate record of the amendment. A covered entity may date and sign an amendment at its discretion.

Comment: The NPRM proposed that covered entities, upon accepting a request for amendment, make reasonable efforts to notify those persons the individual identifies, and other persons whom the covered entity knows have received the erroneous or incomplete information and who may have relied, or could foreseeably rely, on such information to the detriment of the individual. Many commenters argued that this notification requirement was too burdensome and should be narrowed. They expressed concern that covered entities would have to notify anyone who might have received the information, even persons identified by the individual with whom the covered entity had no contact. Other commenters also contended that this provision would require covered entities to determine the reliance another entity might place on the information and suggested that particular part of the notification requirements be removed. Another commenter suggested that the notification provision be eliminated entirely, believing that it was unnecessary.

Response: Although there is some associated administrative burden with this provision, we believe it is a necessary requirement to effectively communicate amendments of erroneous or incomplete information to other parties. The negative effects of erroneous or incomplete medical information can be devastating. This requirement allows individuals to exercise some control in determining recipients they consider important to be notified, and requires the covered entity to communicate amendments to other persons that the covered entity knows have the erroneous or incomplete information and may take some action in reliance on the erroneous or incomplete information to the detriment of the individual. We have added language to clarify that the covered entity must obtain the individual's agreement to have the amendment shared with the persons the individual and covered entity identifies. We believe these notification requirements appropriately balance covered entities' burden and individuals' interest in protecting the accuracy of medical information used to make decisions about them. We therefore retain the notification provisions substantially as proposed.

Comment: Some commenters argued against the proposed provision requiring a covered entity that receives a notice of amendment to notify its business associates, ''as appropriate,'' of necessary amendments. Some argued that covered entities should only be required to inform business associates of these changes if the amendment could affect the individual's further treatment, citing the administrative and financial burden of notifying all business associates of changes that may not have a detrimental effect on the patient. Other commenters suggested that covered entities should only be required to inform business associates whom they reasonably know to be in possession of the information.

Response: We agree with commenters that clarification is warranted. Our intent is that covered entities must meet the requirements of this rule with respect to protected health information they maintain, including protected health information maintained on their behalf by their business associates. We clarify this intent by revising the definition of designated record set (see § 164.501) to include records maintained ''by or for'' a covered entity. Section 164.526(e) requires a covered entity that is informed of an amendment made by another covered entity to incorporate that amendment into designated record sets, whether the designated record set is maintained by the covered entity or for the covered entity by a business associate. If a business associate maintains the record at issue on the covered entity's behalf, the covered entity must fulfill its requirement by informing the business associate of the amendment to the record. The contract with the business associate must require the business associate to incorporate any such amendments. (See § 164.504(e).)

Comment: Some commenters supported the proposal to require covered entities to provide notification of the covered entity's statement of denial and the individual's statement of disagreement in any subsequent disclosures of the information to which the dispute relates. They argued that we should extend this provision to prior recipients of disputed information who have relied on it. These commenters noted an inconsistency in the proposed approach, since notification of accepted amendments is provided to certain previous recipients of erroneous health information and to recipients of future disclosures. They contended there is not a good justification for the different treatment and believed that the notification standard should be the same, regardless of whether the covered entity accepts the request for amendment.

These commenters also recommended that the individual be notified of the covered entity's intention to rebut a statement of disagreement. They suggested requiring covered entities to send a copy of the statement of rebuttal to the individual.

Response: Where a request for amendment is accepted, the covered entity knows that protected health information about the individual is inaccurate or incomplete or the amendment is otherwise warranted; in these circumstances, it is reasonable to ask the covered entity to notify certain previous recipients of the information that reliance on such information could be harmful. Where, however, the request for amendment is denied, the covered entity believes that the relevant information is accurate and complete or the amendment is otherwise unacceptable. In this circumstance, the burden of prior notification outweighs the potential benefits. We therefore do not require notification of prior recipients.

We agree, however, that individuals should know how a covered entity has responded to their requests, and therefore add a requirement that covered entities also provide a copy of any rebuttal statements to the individual.

Section 164.528—Accounting of Disclosures of Protected Health Information

Comment: Many commenters expressed support for the concept of the right to receive an accounting of disclosures. Others opposed even the concept. One commenter said that it is likely that some individuals will request an accounting of disclosures from each of his or her health care providers and payors merely to challenge the disclosures that the covered entity made.

Some commenters also questioned the value to the individual of providing the right to an accounting. One commenter stated that such a provision would be meaningless because those who deliberately perpetrate an abuse are unlikely to note their breach in a log.

Response: The final rule retains the right of an individual to receive an accounting of disclosures of protected health information. The provision serves multiple purposes. It provides a means of informing the individual as to which information has been sent to which recipients. This information, in turn, enables individuals to exercise certain other rights under the rule, such as the rights to inspection and amendment, with greater precision and ease. The accounting also allows individuals to monitor how covered entities are complying with the rule. Though covered entities who deliberately make disclosures in violation of the rule may be unlikely to note such a breach in the accounting, other covered entities may document inappropriate disclosures that they make out of ignorance and not malfeasance. The accounting will enable the individual to address such concerns with the covered entity.

We believe this approach is consistent with well-established privacy principles, with other law, and with industry standards and ethical guidelines. The July 1977 Report of the Privacy Protection Study Commission recommended that a health care provider should not disclose individually-identifiable information for certain purposes without the individual's authorization unless ''an accounting of such disclosures is kept and the individual who is the subject of the information being disclosed can find out that the disclosure has been made and to whom.'' [32] With certain exceptions, the Privacy Act (5 U.S.C. 552a) requires government agencies to ''keep an accurate accounting of * * * the date, nature, and purpose of each disclosure of a record to any person or to another agency * * * and * * * the name and address of the person or agency to whom the disclosure is made.'' The National Association of Insurance Commissioners' Health Information Privacy Model Act requires carriers to provide to individuals on request ''information regarding disclosure of that individual's protected health information that is sufficient to exercise the right to amend the information.'' We build on these standards in this final rule.

Comment: Many commenters disagreed with the NPRM's exception for treatment, payment, and health care operations. Some commenters wanted treatment, payment, and health care operations disclosures to be included in an accounting because they believed that improper disclosures of protected health information were likely to be committed by parties within the entity who have access to protected health information for treatment, payment, and health care operations related purposes. They suggested that requiring covered entities to record treatment, payment, and health care operations disclosures would either prevent improper disclosures or enable transgressions to be tracked.

One commenter reasoned that disclosures for treatment, payment, and health care operations purposes should be tracked since these disclosures would be made without the individual's consent. Others argued that if an individual's authorization is not required for a disclosure, then the disclosure should not have to be tracked for a future accounting to the individual.

One commenter requested that the provision be restated so that no accounting is required for disclosures ''compatible with or directly related to'' treatment, payment or health care operations. This comment indicated that the change would make § 164.515(a)(1) of the NPRM consistent with § 164.508(a)(2)(i)(A) of the NPRM.

Response: We do not accept the comments suggesting removing the exception for disclosures for treatment, payment, and health care operations. While including all disclosures within the accounting would provide more information to individuals about to whom their information has been disclosed, we believe that documenting all disclosures made for treatment, payment, and health care operations purposes would be unduly burdensome on entities and would result in accountings so voluminous as to be of questionable value. Individuals who seek treatment and payment expect that their information will be used and disclosed for these purposes. In many cases, under this final rule, the individual will have consented to these uses and disclosures. Thus, the additional information that would be gained from including these disclosures would not outweigh the added burdens on covered entities. We believe that retaining the exclusion of disclosures to carry out treatment, payment, and health care operations makes for a manageable accounting both from the point of view of entities and of individuals. We have conformed the language in this section with language in other sections of the rule regarding uses and disclosures to carry out treatment, payment, and health care operations. See § 164.508 and the corresponding preamble discussion regarding our decision to use this language.

Comments: A few commenters called for a record of all disclosures, including a right of access to a full audit trail where one exists. Some commenters stated while audit trails for paper records are too expensive to require, the privacy rule should not discourage audit trails, at least for computer-based records. They speculated that an important reason for maintaining a full audit trail is that most abuses are the result of activity by insiders. On the other hand, other commenters pointed out that an enormous volume of records would be created if the rule requires recording all accesses in the manner of a full audit trail.

One commenter supported the NPRM's reference to the proposed HIPAA Security Rule, agreeing that access control and disclosure requirements under this rule should be coordinated with the final HIPAA Security Rule. The commenter recommended that HHS add a reference to the final HIPAA Security Rule in this section and keep specific audit log and reporting requirements generic in the privacy rule.

Response: Audit trails and the accounting of disclosures serve different functions. In the security field, an audit trail is typically a record of each time a sensitive record is altered, how it was altered and by whom, but does not usually record each time a record is used or viewed. The accounting required by this rule provides individuals with information about to whom a disclosure is made. An accounting, as described in this rule, would not capture uses. To the extent that an audit trail would capture uses, consumers reviewing an audit trail may not be able to distinguish between

[32] Privacy Protection Study Commission, ''Personal Privacy in an Information Society,'' July 1977, pp. 306–307.

accesses of the protected health information for use and accesses for disclosure. Further, it is not clear the degree to which the field is technologically poised to provide audit trails. Some entities could provide audit trails to individuals upon their request, but we are concerned that many could not.

We agree that it is important to coordinate this provision of the privacy rule with the Security Rule when it is issued as a final rule.

Comments: We received many comments from researchers expressing concerns about the potential impact of requiring an accounting of disclosures related to research. The majority feared that the accounting provision would prove so burdensome that many entities would decline to participate in research. Many commenters believed that disclosure of protected health information for research presents little risk to individual privacy and feared that the accounting requirement could shut down research.

Some commenters pointed out that often only a few data elements or a single element is extracted from the patient record and disclosed to a researcher, and that having to account for so singular a disclosure from what could potentially be an enormous number of records imposes a significant burden. Some said that the impact would be particularly harmful to longitudinal studies, where the disclosures of protected health information occur over an extended period of time. A number of commenters suggested that we not require accounting of disclosures for research, registries, and surveillance systems or other databases unless the disclosure results in the actual physical release of the patient's entire medical record, rather than the disclosure of discrete elements of information contained within the record.

We also were asked by commenters to provide an exclusion for research subject to IRB oversight or research that has been granted a waiver of authorization pursuant to proposed § 164.510, to exempt ''in-house'' research from the accounting provision, and to allow covered entities to describe the type of disclosures they have made to research projects, without specifically listing each disclosure. Commenters suggested that covered entities could include in an accounting a listing of the various research projects in which they participated during the time period at issue, without regard to whether a particular individual's protected health information was disclosed to the project.

Response: We disagree with suggestions from commenters that an accounting of disclosures is not necessary for research. While it is possible that informing individuals about the disclosures made of their health information may on occasion discourage worthwhile activities, we believe that individuals have a right to know who is using their health information and for what purposes. This information gives individuals more control over their health information and a better base of knowledge from which to make informed decisions.

For the same reasons, we also do not believe that IRB or privacy board review substitutes for providing individuals the right to know how their information has been disclosed. We permit IRBs or privacy boards to determine that a research project would not be feasible if authorization were required because we understand that it could be virtually impossible to get authorization for archival research involving large numbers of individuals or where the location of the individuals is not easy to ascertain. While providing an accounting of disclosures for research may entail some burden, it is feasible, and we do not believe that IRBs or privacy boards would have a basis for waiving such a requirement. We also note that the majority of comments that we received from individuals supported including more information in the accounting, not less.

We understand that requiring covered entities to include disclosures for research in the accounting of disclosures entails some burden, but we believe that the benefits described above outweigh the burden.

We do not agree with commenters that we should exempt disclosures where only a few data elements are released or in the case of data released without individuals' names. We recognize that information other than names can identify an individual. We also recognize that even a few data elements could be clues to an individual's identity. The actual volume of information released is not an appropriate indicator of whether an individual could have a concern about privacy.

We disagree with comments that suggested that it would be sufficient to provide individuals with a general list of research projects to which information has been disclosed by the covered entity. We believe that individuals are entitled to a level of specificity about disclosures of protected health information about them and should know to which research projects their protected health information has been disclosed, rather than to which projects protected health information may have been disclosed. However, we have added a provision allowing for a summary accounting of recurrent disclosures. For multiple disclosures to the same recipient pursuant to a single authorization or for a single purpose permitted under the rule without authorization, the covered entity may provide a summary accounting addressing the series of disclosures rather than a detailed accounting of each disclosure in the series. This change is designed to ease the burden on covered entities involved in longitudinal projects.

With regard to the suggestion that we exempt ''in-house'' research from the accounting provision, we note that only disclosures of protected health information must appear in an accounting.

Comments: Several commenters noted that disclosures for public health activities may be of interest to individuals, but add to the burden imposed on entities. Furthermore, some expressed fear that priority public health activities would be compromised by the accounting provision. One commenter from a health department said that covered entities should not be required to provide an accounting to certain index cases, where such disclosures create other hazards, such as potential harm to the reporting provider. This commenter also speculated that knowing protected health information had been disclosed for these public health purposes might cause people to avoid treatment in order to avoid being reported to the public health department.

A provider association expressed concern about the effect that the accounting provision might have on a non-governmental, centralized disease registry that it operates. The provider organization feared that individuals might request that their protected health information be eliminated in the databank, which would make the data less useful.

Response: As in the discussion of research above, we reject the contention that we should withhold information from individuals about where their information has been disclosed because informing them could occasionally discourage some worthwhile activities. We also believe that, on balance, individuals' interest in having broad access to this information outweighs concerns about the rare instances in which providing this information might raise concerns about harm to the person who made the disclosure. As we stated above, we believe that individuals have

a right to know who is using their health information and for what purposes. This information gives individuals more control over their health information and a better base of knowledge from which to make informed decisions.

Comment: We received many comments about the proposed time-limited exclusion for law enforcement and health oversight. Several commenters noted that it is nearly impossible to accurately project the length of an investigation, especially during its early stages. Some recommended we permit a deadline based on the end of an event, such as conclusion of an investigation. One commenter recommended amending the standard such that covered entities would never be required to give an accounting of disclosures to health oversight or law enforcement agencies. The commenter noted that there are public policy reasons for limiting the extent to which a criminal investigation is made known publicly, including the possibility that suspects may destroy or falsify evidence, hide assets, or flee. The commenter also pointed out that disclosure of an investigation may unfairly stigmatize a person or entity who is eventually found to be innocent of any wrongdoing.

On the other hand, many commenters disagreed with the exemption for recording disclosures related to oversight activities and law enforcement. Many of these commenters stated that the exclusion would permit broad exceptions for government purposes while holding disclosures for private purposes to a more burdensome standard.

Some commenters felt that the NPRM made it too easy for law enforcement to obtain an exception. They suggested that law enforcement should not be excepted from the accounting provision unless there is a court order. One commenter recommended that a written request for exclusion be dated, signed by a supervisory official, and contain a certification that the official is personally familiar with the purpose of the request and the justification for exclusion from accounting.

Response: We do not agree with comments suggesting that we permanently exclude disclosures for oversight or law enforcement from the accounting. We believe generally that individuals have a right to know who is obtaining their health information and for what purposes.

At the same time, we agree with commenters that were concerned that an accounting could tip off subjects of investigations. We have retained a time-limed exclusion period similar to that proposed in the NPRM. To protect the integrity of investigations, in the final rule we require covered entities to exclude disclosures to a health oversight agency or law enforcement official for the time specified by that agency or official, if the agency or official states that including the disclosure in an accounting to the individual would be reasonably likely to impede the agency or official's activities. We require the statement from the agency or official to provide a specific time frame for the exclusion. For example, pursuant to a law enforcement official's statement, a covered entity could exclude a law enforcement disclosure from the accounting for a period of three months from the date of the official's statement or until a date specified in the statement.

In the final rule, we permit the covered entity to exclude the disclosure from an accounting to an individual if the agency or official makes the statement orally and the covered entity documents the statement and the identify of the agency or official that made the statement. We recognize that in urgent situations, agencies and officials may not be able to provide statements in writing. If the agency or official's statement is made orally, however, the disclosure can be excluded from an accounting to the individual for no longer than 30 days from the oral statement. For exclusions longer than 30 days, a covered entity must receive a written statement.

We believe these requirements appropriately balance individuals' rights to be informed of the disclosures of protected health information while recognizing the public's interest in maintaining the integrity of health oversight and law enforcement activities.

Comment: One commenter stated that under Minnesota law, providers who are mandated reporters of abuse are limited as to whom they may reveal the report of abuse (generally law enforcement authorities and other providers only). This is because certain abusers, such as parents, by law may have access to a victim's (child's) records. The commenter requested clarification as to whether these disclosures are exempt from the accounting requirement or whether preemption would apply.

Response: While we do not except mandatory disclosures of abuse from the accounting for disclosure requirement, we believe the commenter's concerns are addressed in several ways. First, nothing in this regulation invalidates or limits the authority or procedures established under state law providing for the reporting of child abuse. Thus, with respect to child abuse the Minnesota law's procedures are not preempted even though they are less stringent with respect to privacy. Second, with respect to abuse of persons other than children, we allow covered entities to refuse to treat a person as an individual's personal representative if the covered entity believes that the individual has been subjected to domestic violence, abuse, or neglect from the person. Thus, the abuser would not have access to the accounting. We also note that a covered entity must exclude a disclosure, including disclosures to report abuse, from the accounting for specified period of time if the law enforcement official to whom the report is made requests such exclusion.

Comment: A few comments noted the lack of exception for disclosures made to intelligence agencies.

Response: We agree with the comments and have added an exemption for disclosures made for national security or intelligence purposes under § 164.512(k)(2). Individuals do not have a right to an accounting of disclosures for these purposes.

Comment: Commenters noted that the burden associated with this provision would, in part, be determined by other provisions of the rule, including the definitions of ''individually identifiable,'' ''treatment,'' and ''health care operations.'' They expressed concern that the covered entity would have to be able to organize on a patient by patient basis thousands of disclosures of information, which they described as ''routine.'' These commenters point to disclosures for patient directory information, routine banking and payment processes, uses and disclosures in emergency circumstances, disclosures to next of kin, and release of admissions statistics to a health oversight agency.

Response: We disagree with the commenters that ambiguity in other areas of the rule increase the burden associated with maintaining an accounting. The definitions of treatment, payment, and health operations are necessarily broad and there is no accounting required for disclosures for these purposes. These terms cover the vast majority of routine disclosures for health care purposes. (See § 164.501 and the associated preamble for a discussion of changes made to these definitions.)

The disclosures permitted under § 164.512 are for national priority purposes, and determining whether a disclosure fits within the section is necessary before the disclosure can be

made. There is no additional burden, once such a determination is made, in determining whether it must be included in the accounting.

We agree with the commenters that there are areas where we can reduce burden by removing additional disclosures from the accounting requirement, without compromising individuals' rights to know how their information is being disclosed. In the final rule, covered entities are not required to include the following disclosures in the accounting: disclosures to the individual, disclosures for facility directories under § 164.510(a), or disclosures to persons assisting in the individual's care or for other notification purposes under § 164.510(b). For each of these types of disclosures, the individual is likely to already know about the disclosure or to have agreed to the disclosure, making the inclusion of such disclosures in the accounting less important to the individual and unnecessarily burdensome to the covered entity.

Comment: Many commenters objected to requiring business partners to provide an accounting to covered entities upon their request. They cited the encumbrance associated with re-contracting with the various business partners, as well as the burden associated with establishing this type of record keeping.

Response: Individuals have a right to know to whom and for what purpose their protected health information has been disclosed by a covered entity. The fact that a covered entity uses a business associate to carry out a function does not diminish an individual's right to know.

Comments: One commenter requested clarification as to how far a covered entity's responsibility would extend, asking whether an entity had to track only their direct disclosures or subsequent re-disclosures.

Response: Covered entities are required to account for their disclosures, as well as the disclosures of their business associates, of protected health information. Because business associates act on behalf of covered entities, it is essential that their disclosures be included in any accounting that an individual requests from a covered entity. Covered entities are not responsible, however, for the actions of persons who are not their business associates. Once a covered entity has accounted for a disclosure to any person other than a business associate, it is not responsible for accounting for any further uses or disclosures of the information by that other person.

Comments: Some commenters said that the accounting provision described in the NPRM was ambiguous and created uncertainty as to whether it addresses disclosures only, as the title would indicate, or whether it includes accounting of uses. They urged that the standard address disclosures only, and not uses, which would make implementation far more practicable and less burdensome.

Response: The final rule requires disclosures, not uses, to be included in an accounting. See § 164.501 for definitions of ''use'' and ''disclosure.''

Comments: We received many comments from providers and other representatives of various segments of the health care industry, expressing the view that a centralized system of recording disclosures was not possible given the complexity of the health care system, in which disclosures are made by numerous departments within entities. For example, commenters stated that a hospital medical records department generally makes notations regarding information it releases, but that these notations do not include disclosures that the emergency department may make. Several commenters proposed that the rule provide for patients to receive only an accounting of disclosures made by medical records departments or some other central location, which would relieve the burden of centralizing accounting for those entities who depend on paper records and tracking systems.

Response: We disagree with commenters' arguments that covered entities should not be held accountable for the actions of their subdivisions or workforce members. Covered entities are responsible for accounting for the disclosures of protected health information made by the covered entity, in accordance with this rule. The particular person or department within the entity that made the disclosure is immaterial to the covered entity's obligation. In the final rule, we require covered entities to document each disclosure that is required to be included in an accounting. We do not, however, require this documentation to be maintained in a central registry. A covered hospital, for example, could maintain separate documentation of disclosures that are made from the medical records department and the emergency department. At the time an individual requests an accounting, this documentation could be integrated to provide a single accounting of disclosures made by the covered hospital. Alternatively, the covered hospital could centralize its processes for making and documenting disclosures. We believe this provision provides covered entities with sufficient flexibility to meet their business needs without compromising individuals' rights to know how information about them is disclosed.

Comments: Commenters stated that the accounting requirements placed undue burden on covered entities that use paper, rather than electronic, records.

Response: We do not agree that the current reliance on paper records makes the accounting provision unduly burdensome. Covered entities must use the paper records in order to make a disclosure, and have the opportunity when they do so to make a notation in the record or in a separate log. We require an accounting only for disclosures for purposes other than treatment, payment, and health care operations. Such disclosures are not so numerous that they cannot be accounted for, even if paper records are involved.

Comments: The exception to the accounting provision for disclosures of protected health information for treatment, payment, and health care operations purposes was viewed favorably by many respondents. However, at least one commenter stated that since covered entities must differentiate between disclosures that require documentation and those that do not, they will have to document each instance when a patient's medical record is disclosed to determine the reason for the disclosure. This commenter also argued that the administrative burden of requiring customer services representatives to ask in which category the information falls and then to keep a record that they asked the question and record the answer would be overwhelming for plans. The commenter concluded that the burden of documentation on a covered entity would not be relieved by the stipulation that documentation is not required for treatment, payment, and health care operations.

Response: We disagree. Covered entities are not required to document every disclosure in order to differentiate those for treatment, payment, and health care operations from those for purposes for which an accounting is required. We require that, when a disclosure is made for which an accounting is required, the covered entity be able to produce an accounting of those disclosures upon request. We do not require a covered entity to be able to account for every disclosure. In addition, we believe that we have addressed many of the commenters' concerns by clarifying in the final rule that disclosures to the

individual, regardless of the purpose for the disclosure, are not subject to the accounting requirement.

Comments: An insurer explained that in the context of underwriting, it may have frequent and multiple disclosures of protected health information to an agent, third party medical provider, or other entity or individual. It requested we reduce the burden of accounting for such disclosures.

Response: We add a provision allowing for a summary accounting of recurrent disclosures. For multiple disclosures to the same recipient pursuant to a single authorization or for a single purpose permitted under the rule without authorization, the covered entity may provide a summary accounting addressing the series of disclosures rather than a detailed accounting of each disclosure in the series.

Comment: Several commenters said that it was unreasonable to expect covered entities to track disclosures that are requested by the individual. They believed that consumers should be responsible for keeping track of their own requests.

Other commenters asked that we specify that entities need not retain and provide copies of the individual's authorization to disclose protected health information. Some commenters were particularly concerned that if they maintain all patient information on a computer system, it would be impossible to link the paper authorization with the patient's electronic records.

Another commenter suggested we allow entities to submit copies of authorizations after the 30-day deadline for responding to the individual, as long as the accounting itself is furnished within the 30-day window.

Response: In the final rule we do not require disclosures to the individual to be included in the accounting. Other disclosures requested by the individual must be included in the accounting, unless they are otherwise excepted from the requirement. We do not agree that individuals should be required to track these disclosures themselves. In many cases, an authorization may authorize a disclosure by more than one entity, or by a class of entities, such as all physicians who have provided medical treatment to the individual. Absent the accounting, the individual cannot know whether a particular covered entity has acted on the authorization.

We agree, however, that it is unnecessarily burdensome to require covered entities to provide the individual with a copy of the authorization. We remove the requirement. Instead, we require the accounting to contain a brief statement describing the purpose for which the protected health information was disclosed. The statement must be sufficient to reasonably inform the individual of the basis for the disclosure. Alternatively, the covered entity may provide a copy of the authorization or a copy of the written request for disclosure, if any, under §§ 164.502(a)(2)(ii) or 164.512.

Comments: We received many comments regarding the amount of information required in the accounting. A few commenters requested that we include additional elements in the accounting, such as the method of transmittal and identity of the employee who accessed the information.

Other commenters, however, felt that the proposed requirements went beyond what is necessary to inform the individual of disclosures. Another commenter stated that if the individual's right to obtain an accounting extends to disclosures that do not require a signed authorization, then the accounting should be limited to a disclosure of the manner and purpose of disclosures, as opposed to an individual accounting of each entity to whom the protected health information was disclosed. An insurer stated that this section of the proposed rule should be revised to provide more general, rather than detailed, guidelines for accounting of disclosures. The commenter believed that its type of business should be allowed to provide general information regarding the disclosure of protected health information to outside entities, particularly with regard to entities with which the insurer maintains an ongoing, standard relationship (such as a reinsurer).

Response: In general, we have retained the proposed approach, which we believe strikes an appropriate balance between the individual's right to know to whom and for what purposes their protected health information has been disclosed and the burden placed on covered entities. In the final rule, we clarify that the accounting must include the address of the recipient only if the address is known to the covered entity. As noted above, we also add a provision allowing for a summary accounting of recurrent disclosures. We note that some of the activities of concern to commenters may fall under the definition of health care operations (see § 164.501 and the associated preamble).

Comment: A commenter asked that we limit the accounting to information pertaining to the medical record itself, as opposed to protected health information more generally. Similarly, commenters suggested that the accounting be limited to release of the medical record only.

Response: We disagree. Protected health information exists in many forms and resides in many sources. An individual's right to know to whom and for what purposes his or her protected health information has been disclosed would be severely limited if it pertained only to disclosure of the medical record, or information taken only from the record.

Comment: A commenter asked that we make clear that only disclosures external to the organization are within the accounting requirement.

Response: We agree. The requirement only applies to disclosures of protected health information, as defined in § 164.501.

Comment: Some commenters requested that we establish a limit on the number of times an individual could request an accounting. One comment suggested we permit individuals to request one accounting per year; another suggested two accountings per year, except in ''emergency situations.'' Others recommended that we enable entities to recoup some of the costs associated with implementation by allowing the entity to charge for an accounting.

Response: We agree that covered entities should be able to defray costs of excessive requests. The final rule provides individuals with the right to receive one accounting without charge in a twelve-month period. For additional requests by an individual within a twelve-month period, the covered entity may charge a reasonable, cost-based fee. If it imposes such a fee, the covered entity must inform the individual of the fee in advance and provide the individual with an opportunity to withdraw or modify the request to avoid or reduce the fee.

Comment: In the NPRM, we solicited comments on the appropriate duration of the individual's right to an accounting. Some commenters supported the NPRM's requirement that the right exist for as long as the covered entities maintains the protected health information. One commenter, however, noted that most audit control systems do not retain data on activity for indefinite periods of time.

Other commenters noted that laws governing the length of retention of clinical records vary by state and by provider type and suggested that entities be allowed to adhere to state laws or policies established by professional organizations or accrediting bodies. Some commenters suggested that the

language be clarified to state that whatever minimum requirements are in place for the record should also guide covered entities in retaining their capacity to account for disclosures over that same time, but no longer.

Several commenters asked us to consider specific time limits. It was pointed out that proposed § 164.520(f)(6) of the NPRM set a six-year time limit for retaining certain information including authorization forms and contracts with business partners. Included in this list was the accounting of disclosures, but this requirement was inconsistent with the more open-ended language in § 164.515. Commenters suggested that deferring to this six-year limit would make this provision consistent with other record retention provisions of the standard and might relieve some of the burden associated with implementation. Other specific time frames suggested were two years, three years, five years, and seven years.

Another option suggested by commenters was to keep the accounting record for as long as entities have the information maintained and ''active'' on their systems. Information permanently taken off the covered entity's system and sent to ''dead storage'' would not be covered. One commenter further recommended that we not require entities to maintain records or account for prior disclosures for members who have ''disenrolled.''

Response: We agree with commenters who suggested we establish a specific period for which an individual may request an accounting. In the final rule, we provide that individuals have a right to an accounting of the applicable disclosures that have been made in the six-year period prior to a request for an accounting. We adopt this time frame to conform with the other documentation retention requirements in the rule. We also note that an individual may request, and a covered entity may then provide, an accounting of disclosures for a period of time less than six years from the date of the request. For example, an individual could request an accounting only of disclosures that occurred during the year prior to the request. In addition, we note that covered entities do not have to account for disclosures that occurred prior to the compliance date of this rule.

Comments: Commenters asked that we provide more time for entities to respond to requests for accounting. Suggestions ranged from 60 days to 90 days. Another writer suggested that entities be able to take up to three 30-day extensions from the original 30-day deadline. Commenters raised concerns about the proposed requirement that a covered health care provider or health plan act as soon as possible.

Response: We agree with concerns raised by commenters and in the final rule, covered entities are required to provide a requested accounting no later than 60 days after receipt of the request. We also provide for one 30 day extension if the covered entity is unable to provide the accounting within the standard time frame. We eliminate the requirement for a covered entity to act as soon as possible.

We recognize that circumstances may arise in which an individual will request an accounting on an expedited basis. We encourage covered entities to implement procedures for handling such requests. The time limitation is intended to be an outside deadline, rather than an expectation. We expect covered entities always to be attentive to the circumstances surrounding each request and to respond in an appropriate time frame.

Comment: A commenter asked that we provide an exemption for disclosures related to computer upgrades, when protected health information is disclosed to another entity solely for the purpose of establishing or checking a computer system.

Response: This activity falls within the definition of health care operations and is, therefore, excluded from the accounting requirement.

Section 164.530—Administrative Requirements

Section 164.530(a)—Designation of a Privacy Official and Contact Person

Comment: Many of the commenters on this topic objected to the cost of establishing a privacy official, including the need to hire additional staff, which might need to include a lawyer or other highly paid individual.

Response: We believe that designation of a privacy official is essential to ensure a central point of accountability within each covered entity for privacy-related issues. The privacy official is charged with developing and implementing the policies and procedures for the covered entity, as required throughout the regulation, and for compliance with the regulation generally. While the costs for these activities are part of the costs of compliance with this rule, not extra costs associated with the designation of a privacy official, we do anticipate that there will be some cost associated with this requirement. The privacy official role may be an additional responsibility given to an existing employee in the covered entity, such as an office manager in a small entity or an information officer or compliance official in a larger institution. Cost estimates for the privacy official are discussed in detail in the overall cost analysis.

Comment: A few commenters argued for more flexibility in meeting the requirement for accountability. One health care provider maintained that covered entities should be able to establish their own system of accountability. For example, most physician offices already have the patient protections incorporated in the proposed administrative requirements—the commenter urged that the regulation should explicitly promote the application of flexibility and scalability. A national physician association noted that, in small offices, in particular, responsibility for the policies and procedures should be allowed to be shared among several people. A major manufacturing corporation asserted that mandating a privacy official is unnecessary and that it would be preferable to ask for the development of policies that are designed to ensure that processes are maintained to assure compliance.

Response: We believe that a single focal point is needed to achieve the necessary accountability. At the same time, we recognize that covered entities are organized differently and have different information systems. We therefore do not prescribe who within a covered entity must serve as the privacy official, nor do we prohibit combining this function with other duties. Duties may be delegated and shared, so long as there is one point of accountability for the covered entity's policies and procedures and compliance with this regulation.

Comment: Some commenters echoed the proposal of a professional information management association that the regulation establish formal qualifications for the privacy official, suggesting that this should be a credentialed information management professional with specified minimum training standards. One commenter emphasized that the privacy official should be sufficiently high in management to have influence.

Response: While there may be some advantages to establishing formal qualifications, we concluded the disadvantages outweigh the advantages. Since the job of privacy official will differ substantially among organizations of varying size and function, specifying a single set of qualifications would sacrifice flexibility and scalability in implementation.

Comment: A few commenters suggested that we provide guidance on the tasks of the privacy official. One noted that this would reduce the burden on covered entities to clearly identify those tasks during the initial HIPAA implementation phase.

Response: The regulation itself outlines the tasks of the privacy official, by specifying the policies and procedures required, and otherwise explaining the duties of covered entities. Given the wide variation in the function and size of covered entities, providing further detail here would unnecessarily reduce flexibility for covered entities. We will, however, provide technical assistance in the form of guidance on the various provisions of the regulation before the compliance date.

Comment: Some comments expressed concern that the regulation would require a company with subsidiaries to appoint a privacy official within each subsidiary. Instead they argued that the corporate entity should have the option of designating a single corporate official rather than one at each subsidiary.

Response: In the final regulation, we give covered entities with multiple subsidiaries that meet the definition of covered entities under this rule the flexibility to designate whether such subsidiaries are each a separate covered entity or are together a single covered entity. (See § 164.504(b) for the rules requiring such designation.) If only one covered entity is designated for the subsidiaries, only one privacy officer is needed. Further, we do not prohibit the privacy official of one covered entity from serving as the privacy official of another covered entity, so long as all the requirements of this rule are met for each such covered entity.

Section 164.530(b)—Training

Comment: A few commenters felt that the proposed provision was too stringent, and that the content of the training program should be left to the reasonable discretion of the covered entity.

Response: We clarify that we do not prescribe the content of the required training; the nature of the training program is left to the discretion of the covered entity. The scenarios in the NPRM preamble of potential approaches to training for different sized covered entities were intended as examples of the flexibility and scalability of this requirement.

Comment: Most commenters on this provision asserted that recertification/retraining every three years is excessive, restrictive, and costly. Commenters felt that retraining intervals should be left to the discretion of the covered entity. Some commenters supported retraining only in the event of a material change. Some commenters supported the training requirement as specified in the NPRM.

Response: For the reasons cited by the commenters, we eliminate the triennial recertification requirements in the final rule. We also clarify that retraining is not required every three years. Retraining is only required in the case of material changes to the privacy policies and procedures of the covered entity.

Comment: Several commenters objected to the burden imposed by required signatures from employees after they are trained. Many commenters suggested that electronic signatures be accepted for various reasons. Some felt that it would be less costly than manually producing, processing, and retaining the hard copies of the forms. Some suggested sending out the notice to the personal workstation via email or some other electronic format and having staff reply via email. One commenter suggested that the covered entity might opt to give web based training instead of classroom or some other type. The commenter indicated that with web based training, the covered entity could record whether or not an employee had received his or her training through the use of a guest book or registration form on the web site. Thus, a physical signature should not be required.

Response: We agree that there are many appropriate mechanisms by which covered entities can implement their training programs, and therefore remove this requirement for signature. We establish only a general requirement that covered entities document compliance with the training requirement.

Comment: Some commenters were concerned that there was no proposed requirement for business associates to receive training and/or to train their employees. The commenters believed that if the business associate violated any privacy requirements, the covered entity would be held accountable. These commenters urged the Secretary to require periodic training for appropriate management personnel assigned outside of the component unit of the covered entity, including business associates. Other commenters felt that it would not be fair to require covered entities to impose training requirements on business associates.

Response: We do not have the statutory authority directly to require business associates to train their employees. We also believe it would be unnecessarily burdensome to require covered entities to monitor business associates' establishment of specific training requirements. Covered entities' responsibility for breaches of privacy by their business associates is described in §§ 164.504(e) and 164.530(f). If a covered entity believes that including a training requirement in one or more of its business associate contracts is an appropriate means of protecting the health information provided to the business associate, it is free to do so.

Comments: Many commenters argued that training, as well as all of the other administrative requirements, are too costly for covered entities and that small practices would not be able to bear the added costs. Commenters also suggested that HHS should provide training materials at little, or no, cost to the covered entity.

Response: For the final regulation, we make several changes to the proposed provisions. We believe that these changes address the issue of administrative cost and burden to the greatest extent possible, consistent with protecting the privacy of health information. In enforcing the privacy rule, we expect to provide general training materials. We also hope to work with professional associations and other groups that target classes of providers, plans and patients, in developing specialized material for these groups.

We note that, under long-standing legal principles, entities are generally responsible for the actions of their workforce. The requirement to train workforce members to implement the covered entity's privacy policies and procedures, and do such things as pass evidence of potential problems to those responsible, is in line with these principles. For example, the comments and our fact finding indicate that, today, many hospitals require their workforce members to sign a confidentiality agreement, and include confidentiality matters in their employee handbooks.

Section 164.530(c)—Safeguards

Comments: A few comments assert that the rule requires some institutions that do not have adequate resources to develop costly physical and technical safeguards without providing a funding mechanism to do so. Another comment said that the vague definitions of adequate and appropriate safeguards could be interpreted by HHS to require the purchase of new computer systems and reprogram many old ones. A few other comments suggested that the safeguards language was vague and asked for more specifics.

Response: We require covered entities to maintain safeguards adequate for their operations, but do not require that

specific technologies be used to do so. Safeguards need not be expensive or high-tech to be effective. Sometimes, it is an adequate safeguard to put a lock on a door and only give the keys to those who need access. As described in more detail in the preamble discussion of § 164.530, we do not require covered entities to guarantee the safety of protected health information against all assaults. This requirement is flexible and scalable to allow implementation of required safeguards at a reasonable cost.

Comments: A few commenters noted that once protected health information becomes non-electronic, by being printed for example, it escapes the protection of the safeguards in the proposed Security Rule. They asked if this safeguards requirement is intended to install similar security protections for non-electronic information.

Response: This provision is not intended to incorporate the provisions in the proposed Security regulation into this regulation, or to otherwise require application of those provisions to paper records.

Comments: Some commenters said that it was unclear what ''appropriate'' safeguards were required by the rule and who establishes the criteria for them. A few noted that the privacy safeguards were not exactly the same as the security safeguards, or that the ''other safeguards'' section was too vague to implement. They asked for more clarification of safeguards requirements and flexible solutions.

Response: In the preamble discussion of § 164.530, we provide examples of types of safeguards that can be appropriate to satisfy this requirement. Other sections of this regulation require specific safeguards for specific circumstances. The discussion of the requirements for ''minimum necessary'' uses and disclosures of protected health information includes related guidance for developing role-based access policies for a covered entity's workforce. The requirements for ''component entities'' include requirements for firewalls to prevent access by unauthorized persons. The proposed Security Rule included further details on what safeguards would be appropriate for electronic information systems. The flexibility and scalability of these rules allows covered entities to analyze their own needs and implement solutions appropriate for their own environment.

Comments: A few comments asked for a requirement for a firewall between a health care component and the rest of a larger organization as another appropriate safeguard.

Response: We agree, and have incorporated such a requirement in § 164.504.

Comments: One commenter agreed with the need for administrative, physical, and technical safeguards, but took issue with our specification of the type of documentation or proof that the covered entity is taking action to safeguard protected health information.

Response: This privacy rule does not require specific forms of proof for safeguards.

Comments: A few commenters asked that, for the requirement for a signed certification of training and the requirements for verification of identity, we consider the use of electronic signatures that meet the requirements in the proposed security regulation to meet the requirements of this rule.

Response: In this final rule, we drop the requirements for signed certifications of training. Signatures are required elsewhere in this regulation, for example, for a valid authorization. In the relevant sections we clarify that electronic signatures are sufficient provided they meet standards to be adopted under HIPAA. In addition, we do not intend to interfere with the application of the Electronic Signature in Global and National Commerce Act.

Comments: A few commenters requested that the privacy requirements for appropriate administrative, technical, and physical safeguards be considered to have been met if the requirements of the proposed Security Rule have been met. Others requested that the safeguards requirements of the final Privacy Rule mirror or be harmonized with the final Security Rule so they do not result in redundant or conflicting requirements.

Response: Unlike the proposed regulation, the final regulation covers all protected health information, not just information that had at some point been electronic. Thus, these commenters' assumption that the proposed Privacy Rule and the proposed Security Rule covered the same information is not the case, and taking the approach suggested by these comments would leave a significant number of health records unprotected. The safeguards required by this regulation are appropriate for both paper and electronic information. We will take care to ensure that the final Security Rule works in tandem with these requirements.

Comments: One commenter requested that the final privacy rule be published before the final Security Rule, recognizing that the privacy policies must be in place before the security technology used to implement them could be worked out. Another commenter asked that the final Security Rule be published immediately and not wait for an expected delay while privacy policies are worked out.

Response: Now that this final privacy rule has been published in a timely manner, the final Security Rule can be harmonized with it and published soon.

Comments: Several commenters echoed an association recommendation that, for those organizations that have implemented a computer based patient record that is compliant with the requirements of the proposed Security Rule, the minimum necessary rule should be considered to have been met by the implementation of role-based access controls.

Response: The privacy regulation applies to paper records to which the proposed Security Rule does not apply. Thus, taking the approach suggested by these comments would leave a significant number of health records unprotected. Further, since the final Security Rule is not yet published and the number of covered entities that have implemented this type of computer-based patient record systems is still small, we cannot make a blanket statement. We note that this regulation requires covered entities to develop role-based access rules, in order to implement the requirements for ''minimum necessary'' uses and disclosures of protected health information. Thus, this regulation provides a foundation for the type of electronic system to which these comments refer.

Section 164.530(d)—Complaints to the Covered Entity

Comment: Several commenters felt that some form of due process is needed when it comes to internal complaints. Specifically, they wanted to be assured that the covered entity actually hears the complaints made by the individual and that the covered entity resolves the complaint within a reasonable time frame. Without due process the commenters felt that the internal complaint process is open ended. Some commenters wanted the final rule to include an appeals process for individuals if a covered entity's determination in regards to the complaint is unfavorable to the individual.

Response: We do not require covered entities to implement any particular due process or appeals process for complaints, because we are concerned about the burden this could impose on covered entities. We provide individuals with an alternative to take their complaints to the Secretary. We believe that this provides incentives for

covered entities to implement a complaint process that resolves complaints to individuals' satisfaction.

Comment: Some commenters felt that the individual making the complaint should exhaust all other avenues to resolve their issues before filing a complaint with the Secretary. A number of commenters felt that any complaint being filed with the Secretary should include documentation of the reviews done by the covered entity.

Response: We reject these suggestions, for two reasons. First, we want to avoid establishing particular process requirements for covered entities' complaint programs. Also, this rule does not require the covered entity to share any information with the complainant, only to document the receipt of the complaint and the resolution, if any. Therefore, we cannot expect the complainant to have this information available to submit to the Secretary. Second, we believe the individual making the complaint should have the right to share the complaint with the Secretary at any point in time. This approach is consistent with existing civil rights enforcement programs for which the Department is responsible. Based on that experience, we believe that most complaints will come first to covered entities for disposition.

Comment: Some commenters wanted the Department to prescribe a minimum amount of time before the covered entity could dispose of the complaints. They felt that storing these complaints indefinitely would be cumbersome and expensive.

Response: We agree, and in the final rule require covered entities to keep all items that must be documented, including complaints, for at least six years from the date of creation.

Comments: Some commenters objected to the need for covered entities to have at least one employee, if not more, to deal with complaints. They felt that this would be costly and is redundant in light of the designation of a contact person to receive complaints.

Response: We do not require assignment of dedicated staff to handle complaints. The covered entity can determine staffing based on its needs and business practices. We believe that consumers need one clear point of contact for complaints, in order that this provision effectively inform consumers how to lodge complaints and so that the compliant will get to someone who knows how to respond. The contact person (or office) is for receipt of complaints, but need not handle the complaints.

Section 164.530(e)—Sanctions

Comment: Commenters argued that most covered entities already have strict sanctions in place for violations of a patient's privacy, either due to current laws, contractual obligations, or good operating practices. Requiring covered entities to create a formal sanctioning process would be superfluous.

Response: We believe it is important for the covered entity to have these sanction policies and procedures documented so that employees are aware of what actions are prohibited and punishable. For entities that already have sanctions policies in place, it should not be problematic to document those policies. We do not define the particular sanctions that covered entities must impose.

Comment: Several commenters agreed that training should be provided and expectations should be clear so that individuals are not sanctioned for doing things that they did not know were wrong or inappropriate. A good faith exception should be included in the final rule to protect these individuals.

Response: We agree that employees should be trained to understand the covered entity's expectations and understand the consequences of any violation. This is why we are requiring each covered entity to train its workforce. However, we disagree that a good faith exception is explicitly needed in the final rule. We leave the details of sanctions policies to the discretion of the covered entity. We believe it is more appropriate to leave this judgment to the covered entity that will be familiar with the circumstances of the violation, rather than to specify such requirements in the regulation.

Comment: Some commenters felt that the sanctions need to reach business partners as well, not just employees of the covered entities. These commenters felt all violators should be sanctioned, including government officials and agencies.

Response: All members of a covered entity's workforce are subject to sanctions for violations, including government officials who are part of a covered entity's workforce. Requirements for addressing privacy violations by business associates are discussed in §§ 164.504(e) and 164.530(f).

Comments: Many commenters appreciated the flexibility left to the covered entities to determine sanctions. However, some were concerned that the covered entity would need to predict each type of violation and the associated sanction. They argue that, if the Department could not determine this in the NPRM, then the covered entities should be allowed to come up with sanctions as appropriate at the time of the violation. Some commenters wanted a better explanation and understanding of what HHS' expectation is of when is it appropriate to apply sanctions. Some commenters felt that the sanctioning requirement is nebulous and requires independent judgment of compliance; as a result it is hard to enforce. Offending individuals may use the vagueness of the standard as an defense.

Response: We agree with the commenters that argue that covered entities should be allowed to determine the specific sanctions as appropriate at the time of the violation. We believe it is more appropriate to leave this judgment to the covered entity, because the covered entity will be familiar with the circumstances of the violation and the best way to improve compliance.

Comment: A commenter felt that the self-imposition of this requirement is an inadequate protection, as there is an inherent conflict of interest when an entity must sanction one of its own.

Response: We believe it is in the covered entity's best interests to appropriately sanction those individuals who do not follow the outlined policies and procedures. Allowing violations to go unpunished may lead bigger problems later, and result in complaints being registered with the Department by aggrieved parties and/or an enforcement action.

Comment: This provision should cover all violations, not just repeat violations.

Response: We do not limit this requirement to repeat offenses.

Section 164.530(f)—Duty To Mitigate

Comments: A few commenters felt that any duty to mitigate would be onerous, especially for small entities. One commenter supported an affirmative duty to mitigate for employees of the covered entity, as long as there is no prescribed mitigation policy. One commenter stated that a requirement for mitigation is unnecessary because any prudent entity would do it.

Some practitioner organizations as well as a health plan, expressed concern about the obligation to mitigate in the context of the business associate relationship. Arguing that it is unnecessary for the regulation to explicitly extend the duty to mitigate to business associates, commenters noted that: Any prudent entity would discipline a vendor or employee that violates a regulation; that the matter is best left to the terms of the contract, and that it is difficult and expensive for a

business associate to have a separate set of procedures on mitigation for each client/provider. One commenter suggested that the federal government should fund the monitoring needed to administer the requirement.

Response: Eliminating the requirement to mitigate harm would undermine the purposes of this rule by reducing covered entities' accountability to their patients for failure to protect their confidential data. To minimize burden, we do not prescribe what mitigation policies and procedures must be implemented. We require only that the covered entity mitigate harm. We also assume that violations will be rare, and so the duty to mitigate harm will rarely be triggered. To the extent a covered entity already has methods for mitigating harm, this rule will not pose significant burden, since we don't require the covered entity to follow any prescribed method or set of rules.

We also modify the NPRM to impose the duty to mitigate only where the covered entity has actual knowledge of harm. Further reducing burden, the rule requires mitigation ''to the extent practicable.'' It does not require the covered entity to eliminate the harm unless that is practicable. For example, if protected health information is advertently provided to a third party without authorization in a domestic abuse situation, the covered entity would be expected to promptly contact the patient as well as appropriate authorities and apprize them of the potential danger.

The harm to the individual is the same, whether the privacy breach was caused by a member of the covered entity's workforce, or by a contractor. We believe the cost of this requirement to be minimal for covered entities that engage in prudent business practices for exchanging protected health information with their business associates.

Comment: A few commenters noted that it is difficult to determine whether a violation has resulted in a deleterious effect, especially as the entity cannot know all places to which information has gone and uses that have been made of it. Consequently, there should be a duty to mitigate even if a deleterious effect cannot be shown, because the individual has no other redress.

Response: As noted above, this provision only applies if the covered entity has actual knowledge of the harm, and requires mitigation ''to the extent practicable.'' The covered entity is expected to take reasonable steps based on knowledge of where the information has been disclosed, how it might be used to cause harm to the patient or another individual, and what steps can actually have a mitigating effect in that specific situation.

Comments: Commenters stated that the language of the regulation was in some places vague and imprecise thus providing covered entities with insufficient guidance and allowing variation in interpretation. Commenters also noted that this could result in inconsistency in implementation as well as permitting such inconsistency to be used as a defense by an offending entity. Particular language for which at least one commenter requested clarification included ''reasonable steps'' and what is entailed in the duty to mitigate.

Response: We considered ways in which we might increase specificity, including defining ''to the extent practicable'' and ''reasonable steps'' and relating the mitigating action to the deleterious impact. While this approach could remove from the covered entity the burden of decision-making about actions that need to be taken, we believe that other factors outweighed this potential benefit. Not only would there be a loss of desirable flexibility in implementation, but it would not be possible to define ''to the extent practicable'' in a way that makes sense for all types of covered entities. We believe that allowing flexibility and judgment by those familiar with the circumstances to dictate the approach is the best approach to mitigating harm.

Section 164.530(g)—Refraining From Intimidating or Retaliatory Acts

Comment: Several commenters stated that the regulation should prohibit covered entities from engaging in intimidating or retaliatory acts against any person, not just against the ''individual,'' as proposed. They suggested adding ''or other person or entity'' after ''any individual.''

Response: We agree, and allow any person to file a compliant with the Secretary. ''Person'' is not limited to natural persons, but includes any type of organization, association or group such as other covered entities, health oversight agencies and advocacy groups.

Comment: A few commenters suggested deleting this provision in its entirety. One commenter indicated that the whistleblower and retaliation provisions could be inappropriately used against a hospital and that the whistleblower's ability to report numerous violations will result in a dangerous expansion of liability. Another commenter stated that covered entities could not take action against an employee who had violated the employer's privacy provisions if this employee files a complaint with the Secretary.

Several commenters suggested deleting ''in any manner'' and ''or opposing any act or practice made unlawful by this subpart'' in § 164.522(d)(4). The commenters indicated that, as proposed, the rule would make it difficult to enforce compliance within the workforce. One commenter stated that the proposed 164.522(d)(4) ''is extremely broad and may allow an employee to reveal protected health information to fellow employees, the media and others (e.g., an employee may show a medical record to a friend or relative before filing a complaint with the Department). This commenter further stated that covered entities will ''absolutely be prevented from prohibiting such conduct.'' One commenter suggested adding that a covered entity may take disciplinary action against any member of its work force or any business partner who uses or discloses individually identifiable health information in violation of this subpart in any manner other than through the processes set forth in the regulation.

Response: To respond to these comments, we make several changes to the proposed provision.

First, where the activity does not involve the filing of a complaint under § 160.306 of this part or participation in an investigation or proceeding initiated by the government under the rule, we delete the phrase ''in any manner'' and add a requirement that the individual's opposition to ''any act or practice'' made unlawful by this subpart be in good faith, and that the expression of that opposition must be reasonable. Second, we add a requirement that the individual's opposition to ''any act or practice'' made unlawful by this subpart must not involve a disclosure of protected health information that is in violation of this subpart. Thus, the employee who discloses protected health information to the media or friends is not protected. In providing interpretations of the retaliation provision, we will consider existing interpretations of similar provisions such as the guidance issued by EEOC in this regard.

Section 164.530(h)—Waiver of Rights

There are no comments directly about this section because it was not included in the proposed rule.

Section 164.530(i)—Policies and Procedures and § 164.530(j)—Documentation Requirements

Comments: Many of the comments to this provision addressed the costs and

complexity of the regulation as a whole, not the additional costs of documenting policies and procedures per se. Some did, either implicitly or explicitly, object to the need to develop and document policies and procedures as creating excessive administrative burden. Many of these commenters also asserted that there is a contradiction between the administrative burden of this provision and one of the statutory purposes of this section of the HIPAA to reduce costs through administrative simplification. Suggested alternatives were generally reliance on existing regulations and ethical standards, or on current business practices.

Response: A specific discussion of cost and burden is found in the Regulatory Impact Analysis of this final rule.

We do not believe there is a contradiction between the administrative costs of this provision and of the goal of administrative simplification. In the Administrative Simplification provisions of the HIPAA, Congress combined a mandate to facilitate the efficiencies and cost savings for the health care industry that the increasing use of electronic technology affords, with a mandate to improve privacy and confidentiality protections. Congress recognized, and we agree, that the benefits of electronic commerce can also cause increased vulnerability to inappropriate access and use of medical information, and so must be balanced with increased privacy protections. By including the mandate for privacy standards in section 264 of the HIPAA, Congress determined that existing regulations and ethical standards, and current business practices were insufficient to provide the necessary protections.

Congress mandated that the total benefits associated with administrative simplification must outweigh its costs, including the costs of implementing the privacy regulation. We are well within this mandate.

Comments: Several commenters suggested that the documentation requirements not be established as a standard under the regulation, because standards are subject to penalties. They recommend we delete the documentation standards and instead provide specific guidance and technical assistance. Several commenters objected to the suggestion in the NPRM that professional associations assist their members by developing appropriate policies for their membership. Several commentators representing professional associations believed this to be an onerous and costly burden for the associations, and suggested instead that we develop specific models which might require only minor modification. Some of these same associations were also concerned about liability issues in developing such guidelines. One commenter argued that sample forms, procedures, and policies should be provided as part of the Final Rule, so that practitioners would not be overburdened in meeting the demands of the regulations. They urged us to apply this provision only to larger entities.

Response: The purpose of requiring covered entities to develop policies and procedures for implementing this regulation is to ensure that important decisions affecting individuals' rights and privacy interests are made thoughtfully, not on an ad hoc basis. The purpose of requiring covered entities to maintain written documentation of these policies is to facilitate workforce training, and to facilitate creation of the required notice of information practices. We further believe that requiring written documentation of key decisions about privacy will enhance accountability, both within the covered entity and to the Department, for compliance with this regulation.

We do not include more specific guidance on the content of the required policies and procedures because of the vast difference in the size of covered entities and types of covered entities' businesses. We believe that covered entities should have the flexibility to design the policies and procedures best suited to their business and information practices. We do not exempt smaller entities, because the privacy of their patients is no less important than the privacy of individuals who seek care from large providers. Rather, to address this concern we ensure that the requirements of the rule are flexible so that smaller covered entities need not follow detailed rules that might be appropriate for larger entities with complex information systems.

We understand that smaller covered entities may require some assistance, and intend to provide such technical assistance after publication of this rule. We hope to work with professional associations and other groups that target classes of providers, plans and patients, in developing specialized material for these groups. Our discussions with several such organizations indicate their intent to work on various aspects of model documentation, including forms. Because the associations' comments regarding concerns about liability did not provide sufficient details, we cannot address them here.

Comment: Many commenters discussed the need for a recognition of scalability of the policies and procedures of an entity based on size, capabilities, and needs of the participants. It was noted that the actual language of the draft regulations under § 164.520 did not address scalability, and suggested that some scalability standard be formally incorporated into the regulatory language and not rely solely on the NPRM introductory commentary.

Response: In § 164.530(i)(1) of the final rule, we specify that we require covered entities to implement policies and procedures that take into account the size of the covered entity and the types of activities that relate to protected health information undertaken by the covered entity.

Comment: One commenter objected to our proposal to allow covered entities to make uses or disclosures not permitted by their current notice if a compelling reason exists to make the use or disclosure and the entity documents the reasons and changes its policies within 30 days of the use or disclosure. The commenter argued that the subjective language of the regulation might give entities the ability to engage in post hoc justifications for violations of their own information practices and policies. The commenter suggested that there should be an objective standard for reviewing the covered entity's reasons before allowing the covered entity to amend its policies.

Response: We eliminate this provision from the final rule. The final rule requires each covered entity to include in its notice of information practices a statement of all permitted uses under this rule, not just those in which the covered entity actually engages in at the time of that notice.

Comment: Some commenters expressed concern that the required retention period in the NPRM applied to the retention of medical records.

Response: The retention requirement of this regulation only applies to the documentation required by the rule, for example, keeping a record of accounting for disclosures or copies of policies and procedures. It does not apply to medical records.

Comments: Comments on the six year retention period were mixed. Some commenters endorsed the six-year retention period for maintaining documentation. One of the comments stated this retention period would assist physicians legally. Other commenters believed that the retention period would be an undue burden. One commenter noted that most State Board of Pharmacy regulations require

pharmacies to keep records for two years, so the six year retention period would triple document retention costs.

Response: We established the retention period at six years because this is the statute of limitations for the civil monetary penalties. This rule does not apply to all pharmacy records, but only to the documentation required by this rule.

Section 164.530(k)—Group Health Plans

There were no comments directly about this section because it was not included in the proposed rule.

Section 164.532—Transition Provisions

Comment: Commenters urged the Department to clarify whether the ''reach of the transition requirement'' is limited to a particular time frame, to the provider's activities in a particular job, or work for a particular employer. For example, one commenter questioned how long a nurse is a covered entity after she moves from a job reviewing files with protected health information to an administrative job that does not handle protected health information; or whether an occupational health nurse who used to transmit first reports of injury to her company's workers' compensation carrier last year but no longer does so this year because of a carrier change still is a covered entity.

Response: Because this comment addresses a question of enforcement, we will address it in the enforcement regulation.

Comment: Several commenters sought clarification as to the application of the privacy rule to research already begun prior to the effective date or compliance date of the final rule. These commenters argued that applying the privacy rule to research already begun prior the rule's effective date would substantially overburden IRBs and that the resulting research interruptions could harm participants and threaten the reliability and validity of conclusions based upon clinical trial data. The commenters recommended that the rule grandfather in any ongoing research that has been approved by and is under the supervision of an IRB.

Response: We generally agree with the concerns raised by commenters. In the final rule, we have provided that covered entities may rely upon consents, authorizations, or other express legal permissions obtained from an individual for a specific research project that includes the treatment of individuals to use or disclose protected health information the covered entity obtained before or after the applicable compliance date of this rule as long as certain requirements are met. These consents, authorizations, or other express legal permissions may specifically permit a use or disclosure of individually identifiable health information for purposes of the project or be a general consent of the individual to participate in the project. A covered entity may use or disclose protected health information it created or received before or after the applicable compliance date of this rule for purposes of the project provided that the covered entity complies with all limitations expressed in the consent, authorization, or permission.

In regard to research projects that include the treatment of individuals, such as clinical trials, covered entities engaged in these projects will have obtained at least an informed consent from the individual to participate in the project. In some cases, the researcher may also have obtained a consent, authorization, or other express legal permission to use or disclose individually identifiable health information in a specific manner. To avoid disrupting ongoing research and because the participants have already agreed to participate in the project (which expressly permits or implies the use or disclosure of their protected health information), we have grandfathered in these consents, authorizations, and other express legal permissions.

It is unlikely that a research project that includes the treatment of individuals could proceed under the Common Rule with a waiver of informed consent. However, to the extent such a waiver has been granted, we believe individuals participating in the project should be able to determine how their protected health information is used or disclosed. Therefore, we require researchers engaged in research projects that include the treatment of individuals who obtained an IRB waiver of informed consent under the Common Rule to obtain an authorization or a waiver of such authorization from an IRB or a privacy board under § 164.512(i) of this rule.

If a covered entity obtained a consent, authorization, or other express legal permission from the individual who is the subject of the research, it would be able to rely upon that consent, authorization, or permission, consistent with any limitations it expressed, to use or disclose the protected health information it created or received prior to or after the compliance date of this regulation. If a covered entity wishes to use or disclose protected health information but no such consent, authorization, or permission exists, it must obtain an authorization pursuant to § 164.508 or obtain a waiver of authorization under § 164.512(i). To the extent such a project is ongoing and the researchers are unable to locate the individuals whose protected health information they are using or disclosing, we believe the IRB or privacy board under the criteria set forth in § 164.512(i) will be able to take that circumstance into account when conducting its review. In most instances, we believe this type of research will be able to obtain a waiver of authorization and be able to continue uninterrupted.

Comment: Several comments raised questions about the application of the rule to individually identifiable information created prior to (1) the effective date of the rule, and (2) the compliance dates of the rule. One commenter suggested that the rule should apply only to information gathered after the effective date of the final rule. A drug manufacturer asked what would be the effect of the rule on research on records compiled before the effective date of the rule.

Response: We disagree with the commenter's suggestion. The requirements of this regulation apply to all protected health information held by a covered entity, regardless of when or how the covered entity obtained the information. Congress required us to adopted privacy standards that apply to individually identifiable health information. While it limited the compliance date for health plans, covered health care providers, and healthcare clearinghouses, it did not provide similar limiting language with regard to individually identifiable health information. Therefore, uses and disclosures of protected health information made by a covered entity after the compliance date of this regulation must meet the requirements of these rules. Uses or disclosures of individually identifiable health information made prior to the compliance date are not affected; covered entities will not be sanctioned under this rule based on past uses or disclosures that are inconsistent with this regulation.

Consistent with the definition of individually identifiable health information in HIPAA, of which protected health information is a subset, we do not distinguish between protected health information in research records and protected health information in other records. Thus, a covered entity's research records are subject to this regulation to the extent they contain protected health information.

Section 164.534—Effective Date and Compliance Date

Section 1175(b)(1)(A) of the Act requires all covered entities other than small health plans to comply with a standard or implementation specification ''not later than 24 months after the date on which an initial standard or implementation specification is adopted or established''; section 1175(b)(1)(B) provides that small health plans must comply not later than 36 months after that date. The proposed rule provided, at proposed § 164.524 (which was titled ''Effective date''), that a covered entity was required to be in compliance with the proposed subpart E not later than 24 months following the effective date of the rule, except that small health plans were required to be in compliance not later than 36 months following the effective date of the rule.

The final rules retain these dates in the text of Subpart E, but denominate them as ''compliance dates,'' to distinguish the statutory dates from the date on which the rules become effective. The effective date of the final rules is 60 days following publication in the **Federal Register.**

Meaning of Effective Date

Comment: A number of commenters expressed confusion about the difference between the effective date of the rule and the effective date on which compliance was required (the statutory compliance dates set out at section 1175(b)(1), summarized above).

Response: The Department agrees that the title of proposed § 164.524 was confusing. Similar comments were received on the Transactions Rule. Those comments were addressed by treating the ''effective date'' of the rule as the date on which adoption takes effect (the ''Effective Date'' heading at the beginning of the preamble), while the dates provided for by section 1175(b)(1) of the statute were denominated as ''compliance dates.'' These changes are reflected in the definition of ''compliance date'' in § 160.103 below (initially published as part of the Transactions Rule) and are also reflected at § 164.524 below. Section 164.524 below has also been reorganized to follow the organization of the analogous provisions of the Transactions Rule. The underlying policy, however, remains as proposed.

Extend the Compliance Date

Comment: Some commenters recommended that the compliance date be extended. A number of comments objected that the time frame for compliance with the proposed standards is unrealistically short. It was pointed out that providers and others would have to do the following, among other things, prior to the applicable compliance date: assess their current systems and departments, determine which state laws were preempted and which were not, update and reprogram computer systems, train workers, create and implement the required privacy policies and procedures, and create or update contracts with business partners. One comment also noted that the task of coming into compliance during the same time period with the other regulations being issued under HIPAA would further complicate the task. These comments generally supported an extension of the compliance dates by one or more years. Other comments supported extending the compliance dates on the ground that the complexity of the tasks involved in implementing the regulation would be a heavy financial burden for providers and others, and that they should be given more time to comply, in order to spread the associated capital and workforce costs over a longer period. It was also suggested that there be provision for granting extensions of the compliance date, based on some criteria, such as a good faith effort to comply or that the compliance dates be extended to two years following completion of a ''state-by-state preemption analysis'' by the Department.

Response: The Secretary acknowledges that covered entities will have to make changes to their policies and procedures during the period between the effective date of the rules below and the applicable compliance dates. The delayed compliance dates which the statute provides for constitute a recognition of the fact changes will be required and are intended to permit covered entities to manage and implement these changes in an orderly fashion. However, because the time frames for compliance with the initial standards are established by statute, the Secretary has no discretion to extend them: Compliance is statutorily required ''not later than'' the applicable compliance date. Nor do we believe that it would be advisable to accomplish this result by delaying the effective date of the final rules beyond 60 days. Since the Transactions Rule is now in effect, it is imperative to bring the privacy protections afforded by the rules below into effect as soon as possible. Retaining the delayed effective date of 60 days, as originally contemplated, will minimize the gap between transactions covered by those rules and not also afforded protection under the rules below.

Phase-in Requirements

Comment: Several comments suggested that the privacy standards be phased in gradually, to ease the manpower and cost burdens of compliance. A couple of equipment manufacturing groups suggested that updating of various types of equipment would be necessary for compliance purposes, and suggested a phased approach to this—for example, an initial phase consisting of preparation of policies, plans, and risk assessments, a second phase consisting of bringing new equipment into compliance, and a final phase consisting of bringing existing equipment into compliance.

Response: As noted in the preceding response, section 1175(b)(1) does not allow the Secretary discretion to change the time frame within which compliance must be achieved. Congress appears to have intended the phasing in of compliance to occur during the two-year compliance period, not thereafter.

Compliance Gap Vis-à-Vis State Laws and Small Health Plans

Comment: Several comments stated that, as drafted, the preemption provisions would be effective as of the rule's effective date (*i.e.,* 60 days following publication), even though covered entities would not be required to comply with the rules for at least another two years. According to these comments, the ''preempted'' state laws would not be in effect in the interim, so that the actual privacy protection would decrease during that period. A couple of comments also expressed concern about how the preemption provisions would work, given the one-year difference in applicable compliance dates for small health plans and other covered entities. A state medical society pointed out that this gap would also be very troublesome for providers who deal with both ''small health plans'' and other health plans. One comment asked what entities that decided to come into compliance early would have to do with respect to conflicting state laws and suggested that, since all parties ''need to know with confidence which laws govern at the moment, * * * [t]here should be uniform effective dates.''

Response: We agree that clarification is needed with respect to the applicability of state laws in the interim between the effective date and the compliance dates. What the comments summarized above appeared to assume is that the preemption provisions of section 1178 operate to broadly and generally invalidate any state law that comes within their ambit. We do not agree that this is the effect of section

1178. Rather, what section 1178 does—where it acts to preempt—is to preempt the state law in question with respect to the actions of covered entities to which the state law applies. Thus, if a provision of state law is preempted by section 1178, covered entities within that state to which the state law applies do not have to comply with it, and must instead comply with the contrary federal standard, requirement, or implementation specification. However, as compliance with the contrary federal standard, requirement, or implementation specification is not required until the applicable compliance date, we do not view the state law in question as meeting the test of being ''contrary.'' That is, since compliance with the federal standard, requirement, or implementation standard is not required prior to the applicable compliance date, it is possible for covered entities to comply with the state law in question. See § 160.202 (definition of ''contrary''). Thus, since the state law is not ''contrary'' to an applicable federal standard, requirement, or implementation specification in the period before which compliance is required, it is not preempted.

Several implications of this analysis should be spelled out. First, one conclusion that flows from this analysis is that preemption is specific to covered entities and does not represent a general invalidation of state law, as suggested by many commenters. Second, because preemption is covered entity-specific, preemption will occur at different times for small health plans than it will occur for all other covered entities. That is, the preemption of a given state law for a covered entity, such as a provider, that is covered by the 24-month compliance date of section 1175(b)(1)(A) will occur 12 months earlier than the preemption of the same state law for a small health plan that is covered by the 36-month compliance date of section 1175(b)(1)(B). Third, the preemption occurs only for covered entities; a state law that is preempted under section 1178(a)(1) would not be preempted for persons and entities to which it applies who are not covered entities. Thus, to the extent covered entities or non-covered entities follow the federal standards on a voluntary basis (*i.e.,* the covered entity prior to the applicable compliance date, the non-covered entity at any time), the state law in question will not be preempted for them.

Small Health Plans

Comment: Several comments, pointing to the ''Small Business'' discussion in the preamble to the proposed rules, applauded the decision to extend the compliance date to three years for small businesses. It was requested that the final rules clarify that the three year compliance date applies to small doctors offices and other small entities, as well as to small health plans.

Response: We recognize that our discussion in the preamble to the proposed rules may have suggested that more covered entities came within the 36 month compliance date than is in fact the case. Again, this is an area in which we are limited by statute. Under section 1175(b) of the Act, only small health plans have three years to come into compliance with the standards below. Thus, other ''small businesses'' that are covered entities must comply by the two-year compliance date.

Coordination With the Security Standard

Comment: Several comments suggested that the security standard be issued either with or after the privacy standards. It was argued that both sets of standards deal with protecting health information and will require extensive personnel training and revisions to business practices, so that coordinating them would make sense. An equipment manufacturers group also pointed out that it would be logical for covered entities and their business partners to know what privacy policies are required in purchasing security systems, and that ''the policies on privacy are implemented through the security standards rather than having already finalized security standards drive policy.''

Response: We agree with these comments, and are making every effort to coordinate the final security standards with the privacy standards below. The privacy standards below are being published ahead of the security standards, which is also responsive to the stated concerns.

Prospective Application

Comment: Several comments raised questions about the application of the rule to individually identifiable information created prior to (1) the effective date of the rule, and (2) the compliance dates of the rule. One provider group suggested that the rule should apply only to information gathered after the effective date of the final rule. A drug manufacturer asked what would be the effect of the rule on research on records compiled before the effective date of the rule.

Response: These comments are addressed in connection with the discussion of § 164.532 above.

Impact Analyses

Cost/Benefit Analysis

Comment: Many commenters made general statements to the effect that the cost estimates for implementing the provisions of the proposed regulation were incomplete or greatly understated.

Response: The proposal, including the cost analysis, is, in effect, a first draft. The purpose of the proposal was to solicit public comment and to use those comments to refine the final regulation. As a result of the public comment, the Department has significantly refined our initial cost estimates for implementing this regulation. The cost analysis below reflects a much more complete analysis of the major components of the regulation than was presented in the proposal.

Comment: Numerous commenters noted that significant areas of potential cost had not been estimated and that if they were estimated, they would greatly increase the total cost of the regulation. Potential cost areas identified by various respondents as omitted from the analyses include the minimum disclosure requirements; the requisite monitoring by covered entities of business partners with whom they share private health information; creation of de-identified information; internal complaint processes; sanctions and enforcement; the designation of a privacy official and creation of a privacy board; new requirements for research/optional disclosures; and future litigation costs.

Response: We noted in the proposed rule that we did not have data from which to estimate the costs of many provisions, and solicited comments providing such data. The final analysis below reflects the best estimate possible for these areas, based on the information available. The data and the underlying assumptions are explained in the cost analysis section below.

Comment: A number of comments suggested that the final regulation be delayed until more thorough analyses could be undertaken and completed. One commenter stated that the Department should refrain from implementing the regulation until a more realistic assessment of costs could be made and include local governments in the process. Similarly, a commenter requested that the Department assemble an outside panel of health industry experts, including systems analysts, legal counsel, and management consultants to develop stronger estimates.

Response: The Department has engaged in extensive research, data collection and fact-finding to improve

the quality of its economic analysis. This has included comments from and discussions with the kinds of experts one commenter suggested. The estimates represent a reasonable assessment of the policies proposed.

Comment: Several commenters indicated that the proposed regulation would impose significant new costs on providers' practices. Furthermore, they believe that it runs counter to the explicit statutory intent of HIPAA's Administrative Simplification provisions which require that ''any standard adopted * * * shall be consistent with the objective of reducing the administrative costs of providing and paying for health care.''

Response: As the Department explained in the Transactions Rule, this provision applies to the administrative simplification regulations of HIPAA in the aggregate. The Transactions Rule is estimated to save the health care system $29.9 billion in nominal dollars over ten years. Other regulations published pursuant to the administrative simplification authority in HIPAA, including the privacy regulation, will result in costs, but these costs are within the statutory directive so long as they do not exceed the $29.9 billion in estimated savings. Furthermore, as explained in the Transactions Rule, and the preamble to this rule, assuring privacy is essential to sustaining many of the advances that computers will provide. If people do not have confidence that their medical privacy will be protected, they will be much less likely to allow their records to be used for any purpose or might even avoid obtaining necessary medical care.

Comment: Several commenters criticized the omission of aggregate, quantifiable benefit estimates in the proposed rule. Some respondents argued that the analysis in the proposed rule used ''de minimis'' cost estimates to argue only that benefits would certainly exceed such a low barrier. These commenters further characterized the benefits analysis in the Notice of Proposed Rulemaking as ''hand waving'' used to divert attention from the fact that no real cost-benefit comparison is presented. Another commenter stated that the benefit estimates rely heavily on anecdotal and unsubstantiated inferences. This respondent believes that the benefit estimates are based on postulated, but largely unsubstantiated causal linkages between increased privacy and earlier diagnosis and medical treatment.

Response: The benefits of privacy are diffused and intangible but real. Medical privacy is not a good people buy or sell in a market; therefore, it is very difficult to quantify. The benefits discussion in the proposal reflects this difficulty. The examples presented in the proposal were meant to be illustrative of the benefits based on a few areas of medicine where some relevant data was available. Unfortunately, no commenters provided either a better methodological approach or better data for assessing the overall benefits of privacy. Therefore, we believe the analysis in the proposal represents a valid illustration of the benefits of privacy, and we do not believe it is feasible to provide an overall dollar estimate of the benefits of privacy in the aggregate.

Comment: One commenter criticized the benefit analysis as being incomplete because it did not consider the potential cost of new treatments that might be engendered by increased confidence in medical privacy resulting from the regulation.

Response: There is no data or model to reliably assess such long-term behavioral and scientific changes, nor to determine what portion of the increasingly rapid evolution of new improved treatments might stem from improved privacy protections. Moreover, to be complete, such analysis would have to include the savings that might be realized from earlier detection and treatment. It is not possible at this time to project the magnitude or even the direction of the net effects of the response to privacy that the commenter suggests.

Scope of the Regulation

Comment: Numerous commenters noted the potential cost and burden of keeping track in medical records of information which had been transmitted electronically, which would be subject to the rule, as opposed to information that had only been maintained in paper form.

Response: This argument was found to have considerable merit and was one of the reasons that the Department concluded that the final regulation should apply to all medical records maintained by covered entities, including information that had never been transmitted electronically. The costs analysis below reflects the change in scope.

Notice Requirements

Comment: Several commenters expressed their belief that the administrative and cost burdens associated with the notice requirements were understated in the proposed rule. While some respondents took issue with the policy development cost estimates associated with the notice, more were focused on its projected implementation and production costs. For example, one respondent stated that determining ''first service'' would be an onerous task for many small practices, and that provider staff will now have to manually review each patient's chart or access a computer system to determine whether the patient has been seen since implementation of the rule.

Response: The policy in the final rule has been changed to make the privacy policy notice to patients less burdensome. Providers will be able to distribute the notice when a patient is seen and will not have to distribute it to a patient more than once, unless substantive changes are made in the notice. This change will significantly reduce the cost of distributing the privacy notices.

Comment: Some commenters also took issue with the methodology used to calculate the cost estimates for notices. These respondents believe that the survey data used in the proposed rule to estimate the costs (*i.e.,* ''encounters,'' ''patients,'' and ''episodes'' per year) are very different concepts that, when used together, render the purported total meaningless. Commenters further stated that they can verify the estimate of 543 million patients cited as being seen at least once every five years.

Response: In the course of receiving treatment, a patient may go to a number of medical organizations. For example, a person might see a doctor in a physician's office, be admitted to a hospital, and later go to a pharmacy for medication. Each time a person ''encounters'' a facility, a medical record may be started or additions made to an existing record. The concept in the proposal was to identify the number of record sets that a person might have for purposes of estimating notice and copying costs. For example, whether a person made one or ten visits in the course of a year to a specific doctor would, for our purposes, be one record set because in each visit the doctor would most likely be adding information to an existing medical record. The comments demonstrated that we had not explained the concept well. As explained below we modified the concept to more effectively measure the number of record sets that exist and explain it more clearly.

Comment: Several commenters criticized the lack of supporting evidence for the cost estimates of notice development and dissemination. Another opinion voiced in the comments is that the estimated cost for plans of $0.75 per insured person is so low that it may cover postage, but it

cannot include labor and capital usage costs.

Response: Based on comments and additional fact finding, the Department was able to gain a better understanding of how covered entities would develop policies and disseminate information. The cost analysis below explains more fully how we derived the final cost estimates for these areas.

Comment: A commenter noted that privacy policy costs assume that national associations will develop privacy policies for members but HHS analysis does not account for the cost to the national associations. A provider cost range of $300–$3,000 is without justification and seems low.

Response: The cost to the national associations was included in the proposal estimates, and it is included in the final analysis (see below).

Comment: A commenter states that the notice costs discussion mixes the terms ''patients'', ''encounters'' and ''episodes'' and 397 million encounter estimate is unclear.

Response: A clearer explanation of the concepts employed in this analysis is provided below.

Systems Compliance Costs

Comment: Numerous commenters questioned the methodology used to estimate the systems compliance cost and stated that the ensuing cost estimates were grossly understated. Some stated that the regulation will impose significant information technology costs to comply with requirement to account for disclosures, additional costs for hiring new personnel to develop privacy policies, and higher costs for training personnel.

Response: Significant comments were received regarding the cost of systems compliance. In response, the Department retained the assistance of consultants with extensive expertise in health care information technology. We have relied on their work to revise our estimates, as described below. The analysis does not include ''systems compliance'' as a cost item, per se. Rather, in the final analysis we organized estimates around the major policy provisions so the public could more clearly see the costs associated with them. To the extent that the policy might require systems changes (and a number of them do), we have incorporated those costs in the provision's estimate.

Comment: Items explicitly identified by commenters as significantly adding to systems compliance costs include tracking disclosures of protected health information and patient authorizations; restricting access to the data; accommodating minimum disclosure provisions; installing notices and disclaimers; creating de-identified data; tracking uses of protected health information by business partners; tracking amendments and corrections; increased systems capacity; and annual systems maintenance. The commenters noted that some of the aforementioned items are acknowledged in the proposed rule as future costs to covered entities, but several others are singularly ignored.

Response: The Department recognizes the validity of much of this criticism. Unfortunately, other than general criticism, commenters provided no specific data or methodological information which might be used to improve the estimates. Therefore, the Department retained consultants with extensive expertise in these areas to assess the proposed regulation, which helped the Department refine its policies and cost estimates.

In addition, it is important to note that the other HIPAA administrative simplification regulations will require systems changes. As explained generally in the cost analysis for the electronic Transactions rule, it is assumed that providers and vendors will undertake systems changes for these regulations collectively, thereby minimizing the cost of changes.

Inspection and Copying

Comment: Numerous commenters disagreed with the cost estimates in the NPRM for inspection and copying of patient records, believing that they were too low.

Response: The Department has investigated the potential costs through a careful reading of the comments and subsequent factfinding discussions with a variety of providers. We believe the estimates, explained more fully below, represent a reasonable estimate in the aggregate. It is important to note, however, that this analysis is not measuring the cost of all inspection and copying because a considerable amount of this already occurs. The Department is only measuring the incremental increase likely to occur as a result of this regulation.

Comment: One commenter speculates that, even at a minimum charge of $.50/page, (and not including search and retrieval charges), costs could run as high as $450 million annually.

Response: The $0.50 per page in the proposal represent an average of several data sources. Subsequently, an industry commenter, which provided extensive medical records copying, stated that this was a reasonable average cost. Hence, we retained the number for the final estimate.

Comment: One respondent states that, since the proposed rules give patients the right to inspect and copy their medical records regardless of storage medium, HHS must make a distinction in its cost estimates between records stored electronically and those which must be accessed by manual means, since these costs will differ.

Response: The cost estimates made for regulations are not intended to provide such refined gradations; rather, they are intended to show the overall costs for the regulation as a whole and its major components. For inspections and copying (and virtually all other areas for which estimates are made) estimates are based on averages; particular providers may experience greater or lesser costs than the average cost used in this analysis.

Comment: Several commenters noted that the Department did not appear to include the cost of establishing storage systems, retrieval fees and the cost of searching for records, and that these costs, if included, would significantly increase the Department's estimate.

Response: Currently, providers keep and maintain medical records and often provide copies to other providers and patients. Therefore, much of the cost of maintaining records already exists. Indeed, based on public comments, the Department has concluded that there will be relatively few additional copies requested as the result of this regulation (see below). We have measured and attributed to this regulation the incremental cost, which is the standard for conducting this kind of analysis.

Comment: A federal agency expressed concern over the proposal to allow covered entities to charge a fee for copying personal health information based on reasonable costs. The agency requests personal health information from many covered entities and pays a fee that it establishes. Allowing covered entities to establish the fee, the agency fears, may cost them significantly more than the current amounts they pay and as a result, could adversely affect their program.

Response: The proposal and the final rule establish the right to access and copy records only for individuals, not other entities; the ''reasonable fee'' is only applicable to the individual's request. The Department's expectation is that other existing practices regarding fees, if any, for the exchange of records not requested by an individual will not be affected by this rule.

Appending Records (Amendment and Correction)

Comment: The proposed rule estimated the cost of amending and correcting patients' records at $75 per instance and $260 million per year for small entities. At least one commenter stated that such requests will rise significantly upon implementation of the regulations and increase in direct proportion to the number of patients served. Another commenter described the more subtle costs associated with record amendment and correction, which would include a case-by-case clinical determination by providers on whether to grant such requests, forwarding the ensuing record changes to business partners, and issuing written statements to patients on the reasons for denials, including a recourse for complaints.

Response: The comments were considered in revising the proposal, and the decision was made to clarify in the final regulation that providers must only append the record (the policy is explained further in the preamble and the regulation text). The provider is now only required to note in the medical record any comments from the patient; they may, but are not required to, correct any errors. This change in policy significantly reduces the cost from the initial proposal estimate.

Comment: Several commenters criticized the proposed rule's lack of justification for assumptions regarding the percentage of patients who request inspection and copying, who also request amendment and correction. Another commenter pointed out that the cost estimate for amendment and correction is dependent on a base assumption that only 1.5 percent of patients will request inspection of their records. As such, if this estimate were too low by just one percentage point, then the estimates for inspection and copying plus the costs for amendment and correction could rise by 67 percent.

Response: Based on information and data received in the public comments, the estimate for the number of people requesting inspection and copying has been revised. No commenter provided specific information on the number of amended record requests that might result, but the Department subsequently engaged in fact-finding and made appropriate adjustments in its estimates. The revisions are explained further below.

Consent and Authorizations

Comment: One respondent indicated that the development, collection, and data entry of all the authorizations will create a new transaction type for employers, health plans, and providers, and result in duplicated efforts among them. This commenter estimates that the costs of mailing, re-mailing, answering inquiries, making outbound calls and performing data entry in newly created authorization computer systems could result in expenses of close to $2.0 billion nationally. Another commenter indicated that authorization costs will be at least double the notice dissemination costs due to the cost of both outbound and return postage.

Response: Public commenters and subsequent factfinding clearly indicate that most providers with patient contact already obtain authorizations for release of records, so for them there is virtually no new cost. Further, this comment does not reflect the actual regulatory requirement. For example, there is no need to engage in mailing and re-mailing of forms, and we do not foresee any reason why there should be any significant calls involved.

Comment: A commenter criticized the percentage (1%) that we used to calculate the number of health care encounters expected to result in requests to withhold the release of protected information. This respondent postulates that even if one in six patients who encounter the U.S. health care system opt to restrict access to their records, the total expected national cost per year could rise to $900 million.

Response: The final regulation requirements regarding the release of protected health information has been substantially changed, thereby greatly reducing the potential cost burden. A fuller explanation of the cost is provided below in the regulatory impact analysis.

Comment: An additional issue raised by commenters was the added cost of seeking authorizations for health promotion and disease management activities, health care operations that traditionally did not require such action.

Response: In the final regulation, a covered entity can use medical information collected for treatment or operations for its own health promotion and disease management efforts without obtaining additional authorization. Therefore, there is no additional cost incurred.

Business Associates

Comment: A number of commenters were concerned about the cost of monitoring business partners. Specifically, one commenter stated that the provisions of the proposed regulation pertaining to business partners would likely force the discontinuation of outsourcing for some functions, thereby driving up the administrative cost of health care.

Response: The final regulation clarifies the obligations of the business associates in assuring privacy. As explained in the preamble, business associates must take reasonable steps to assure confidentiality of health records they may have, and the covered entity must take appropriate action if they become aware of a violation of the agreement they have with the business associate. This does not represent an unreasonable burden; indeed, the provider is required to take the same kind of precautions and provide the same kind of oversight that they would in many other kinds of contractual relationships to assure they obtain the quality and level of performance that they would expect from a business associate.

Comment: HHS failed to consider enforcement costs associated with monitoring partners and litigation costs arising from covered entities seeking restitution from business partners whose behavior puts the covered entity at risk for noncompliance.

Response: The Department acknowledged in the proposal that it was not estimating the cost of compliance with the business associates provision because of inadequate information. It requested information on this issue, but no specific information was provided in the comments. However, based on revisions in the final policy and subsequent factfinding, the Department has provided an estimate for this requirement, as explained below.

Training

Comment: Many of the commenters believe that the Department used unrealistic assumptions in the development of the estimated cost of the training provisions and they provided their own estimates.

Response: The commenters' estimates varied widely, and could not be used by the Department in revising its analysis because there was inadequate explanation of how the estimates were made.

Comment: Several commenters argued that if even an hour of time of each of the entity's employees is spent on training instead of ''work'' and they are paid the minimum wage, an entity would incur $100 of cost for training no more than 20 employees. The commenters noted that the provision of health care services is a labor-intensive enterprise, and many covered entities have thousands of employees, most of whom make well in excess of minimum

wage. They questioned whether the estimates include time taken from the employee's actual duties (opportunity cost) and the cost of a trainer and materials.

Response: As explained in more detail below, the Department made extensive revisions in its training estimate, including the number of workers in the health care sector, the cost of workers in training based on average industry wages, and training costs (instructors and materials). The revised estimate is a more complete and accurate estimate of the costs likely to be borne as a result of the final regulation.

Comment: One commenter estimated that simply training an employee could have a burdensome impact on his company. He argued, for example, a 10-hour annual requirement takes 0.5% of an employee's time if they work a 2000-hour year, but factoring in sick and vacation leave, the effects of industry turnover could significantly increase the effect.

Response: In the analysis below, the Department has factored in turnover rates, employment growth and greater utilization based on data obtained from broad-based surveys and a public comment.

Comment: Some commenters felt that the regulatory training provisions are overly burdensome. Specific concerns centered around the requirement to train all individuals who may come in contact with protected health information and the requirement to have such individuals sign a new certifying statement at least every three years. Some commenters felt that the content of the training program should be left to the discretion of the covered entity.

Response: Changes and clarifications in the training requirements are made in the final regulation, explained below. For example, the certification requirement has been eliminated. As in the NPRM, the content of the training program is left to the discretion of the covered entity. These changes are expected to lessen the training burden and are reflected in the final cost estimates.

Compliance and Enforcement

Comment: A Member of Congress and a number of privacy and consumer groups expressed their concern with whether the Office for Civil Rights (OCR) in HHS has adequate funding to carry out the major responsibility of enforcing the complaint process established by this rule. The Member stated that ''[d]ue to the limited enforcement ability allowed for in this rule by HIPAA, it is essential that OCR have the capacity to enforce the regulations. Now is the time for The Secretary to begin building the necessary infrastructure to enforce the regulation effectively.''

Response: The Secretary agrees with the commenters and is committed to an effective enforcement program. We will work with Congress to ensure that the Department has the necessary funds to secure voluntary compliance through education and technical assistance, to investigate complaints and conduct compliance reviews, to provide states with exception determinations and to use civil and criminal penalties when necessary.

Economic Effect on Small Entities

Comment: Many commenters stated that the cost estimates on the effect of the proposed regulation on small businesses were understated or incomplete.

Response: The Department conducted a thorough review of potential data sources that would improve the quality of the analysis of the effects on small business. The final regulatory flexibility analysis below is based on the best data available (much of it from the Small Business Administration) and represents a reliable estimate for the effects on small entities in various segments of the health care industry. It is important to note that the estimates are for small business segments in the aggregate; the cost to individual firms will vary, perhaps considerably, based on its particular circumstances.

Comment: The cost of implementing privacy regulations, when added to the cost of other required HIPAA regulations, could increase overhead significantly. As shown in the 1993 Workgroup on Electronic Data Interchange (WEDI) Report, providers will bear the larger share of implementation costs and will save less than payors.

Response: The regulatory flexibility analysis below shows generally the marginal effect of the privacy regulation on small entities. Collectively, the HIPAA administrative standards will save money in the health care system. As important, given the rapid expansion of electronic commerce, it is probable that small entities would need to comply with standards for electronic commerce in order to complete effectively, even if the standards were voluntary. The establishment of uniform standards through regulation help small entities because they will not have to invest in multiple systems, which is what they would confront if the system remained voluntary.

Comment: One respondent believed that the initial and ongoing costs for small provider offices could be as much as 11 times higher than the estimates provided in the proposed rule. Other commenters stated that the estimates for small entities are ''absurdly low''.

Response: Although there were a number of commenters highly critical of the small business analysis, none provided alternative estimates or even provided a rationale for their statements. Many appeared to assume that all costs associated with medical record confidentiality should be estimated. This represents a misunderstanding of the purpose of the analysis: to estimate the incremental effects of this regulation, *i.e.,* the new costs (and savings) that will result from changes required by the regulation. The Department has made substantial changes in the final small entities analysis (below), reflecting policy changes in the final rule and additional information and data collected by the Department since the issuance of the proposal last fall. We believe that these estimates reasonably reflect the costs that various types of small entities will experience in general, though the actual costs of particular providers might vary considerably based on their current practices and technology.

Comment: A respondent expressed the belief that small providers would bear a disproportionate share of the regulation's administrative burden because of the likelihood of larger companies incurring fewer marginal costs due to greater in-house resources to aid in the legal and technical analysis of the proposed rule.

Response: As explained below, the Department does not agree with the assertion that small entities will be disproportionately affected. Based on discussions with a number of groups, the Department expects many professional and trade associations to provide their members with analysis of the regulation, including model policies, statements and basic training materials. This will minimize the cost for most small entities. Providers that use protected health information for voluntary practices, such as marketing or research, are more likely to need specific legal and technical assistance, but these are likely to be larger providers.

Comment: Several commenters took issue with the ''top-down'' approach that we used to estimate costs for small businesses, believing that this methodology provided only a single point estimate, gave no indication of the variation around the estimate, and was subject to numerous methodological errors since the entities to which the numerator pertained may not have been

the same as the denominator. These respondents further recommended that we prepare a ''bottom-up'' analysis using case studies and/or a survey of providers to refine the estimates.

Response: The purpose of the regulatory flexibility analysis is to provide a better insight into the relative burden of small businesses compared to larger firms in complying with a regulation. There may be considerable variance around average costs within particular industry sectors, even among small businesses within them. The estimates are based on the best data available, including information from the Small Business Administration, the Census Bureau, and public comments.

Comment: A commenter stated that the proposal's cost estimate does not account for additional administrative costs imposed on physicians, such as requirements to rewrite contracts with business partners.

Response: Such costs are included in the analysis below.

Comment: Numerous public comments were directed specifically at the systems compliance cost estimates for small businesses. One respondent maintained that the initial upgrade cost alone would range from $50 thousand to more than $1 million per covered entity.

Response: The cost estimates for systems compliance varied enormously; unfortunately, none of the commenters provided documentation of how they made their estimates, preventing us from comparing their data and assumptions to the Department's. Because of concern about the costs in this area, however, the Department retained an outside consultant to provide greater expertise and analysis. The product of this effort has been incorporated in the analysis below.

Comment: One commenter stated that just the development and documentation of new health information policies and procedures (which would require an analysis of the federal regulations and state law privacy provisions), would cost far more than the $396 cited in the Notice of Proposed Rulemaking as the average start-up cost for small businesses.

Response: As explained below in the cost analysis, the Department anticipates that most of the policies and procedures that will be required under the final rule will be largely standardized, particularly for small businesses. Thus, much of the work and cost can be done by trade associations and professional groups, thereby minimizing the costs and allowing it to be spread over a large membership base.

Comment: A number of comments criticized the initial estimates for notices, inspection and copying, amendments and correction, and training as they relate to small businesses.

Response: The Department has made substantial revisions in its estimates for all of these areas which is explained below in the regulatory flexibility analysis.

Comment: One commenter noted that there appeared to be a discrepancy in the number of small entities cited. There is no explanation for the difference and no explanation for difference between ''establishments'' and ''entities.''

Response: There are discrepancies among the data bases on the number of ''establishments'' and ''entities'' or ''firms''. The problem arises because most surveys count (or survey) establishments, which are physical sites. A single firm or entity may have many establishments. Moreover, although an establishment may have only a few employees, the firm may have a large number of workers (the total of all its various establishments) and therefore not be a small entity.

As discussed below, there is some discrepancy between the aggregate numbers we use for the regulatory impact analysis (RIA) and the regulatory flexibility analysis (RFA). We concluded that for purposes of the RFA, which is intended to measure the effects on small entities, we would use Small Business Administration data, which defines entities based on revenues rather than physical establishments to count the number of small entities in various SIC. This provides a more accurate estimate of small entities affected. For the RIA, which is measuring total effects, we believe the establishment based surveys provide a more reliable count.

Comment: Because small businesses must notify patients of their privacy policies on patients' first visit after the effective date of the regulation, several commenters argued that staff would have to search records either manually or by computer on a daily basis to determine if patients had been seen since the regulation was implemented.

Response: Under the final regulation, all covered entities will have to provide patients copies of their privacy policy at the first visit after the effective date of the regulation. The Department does not view this as burdensome. We expect that providers will simply place a note or marker at the beginning of a file (electronic or paper) when a patient is given the notice. This is neither time-consuming nor expensive, and it will not require constant searches of records.

Comment: A commenter stated that the definitions of small business, small entity, and a small health plan are inconsistent because the NPRM includes firms with annual receipts of $5 million or less and non-profits.

Response: The Small Business Administration, whose definitions we use for this analysis, includes firms with $5 million or less in receipts and all non-profits as ''small businesses.'' We recognize that some health plans, though very large in terms of receipts (and insured lives), nonetheless would be considered ''small businesses'' under this definition because they are non-profits. In the final regulatory flexibility analysis, we generally have maintained the Small Business Administration definitions because it is the accepted standard for these analyses. However, we have added several categories, such as IRBs and employer sponsored group health plans, which are not small entities, per se, but will be effected by the final rule and we were able to identify costs imposed by the regulation on them.

Comment: The same commenter wanted clarification that all non-profit organizations are small entities and that the extended effective date for compliance applies to them.

Response: For purposes of the regulatory flexibility analysis, the Department is utilizing the Small Business Administration guidelines. However, under HIPAA the Secretary may extend the effective compliance date from 24 months to 36 months for ''small health plans''. The Secretary is given the explicit discretion of defining the term for purposes of compliance with the regulation. For compliance purposes, the Secretary has decided to define ''small health plans'' as those with receipts of $5 million or less, regardless of their tax status. As noted above, some non-profit plans are large in terms of revenues (*i.e.,* their revenues exceed $5 million annually). The Department determined that such plans do not need extra time for compliance.

Comment: Several commenters requested that ''small providers'' [undefined] be permitted to take 36 months to come into compliance with the final regulation, just as small health plans will be permitted to do so.

Response: Congress specified small health plans, but not small providers, as needing extra time to comply. The majority of providers affected by the regulation are ''small'', based on the SBA definitions; in other words, granting the delay would be tantamount to make the effective date three years rather than two. In making policy decisions for the final regulation, extensive consideration was given to minimizing the cost and administrative burden associated with implementing

the rule. The Department believes that the requirements of the final rule will not be difficult to fulfill, and therefore, it has maintained the two year effective date.

External Studies

Comment: One commenter submitted a detailed analysis of privacy legislation that was pending and concluded that they might cost over $40 billion.

Response: The study did not analyze the policies in the proposal, and therefore, the estimates do not reflect the costs that would have been imposed by the proposed regulation. In fact, the analysis was prepared before the Administration's proposed privacy regulation was even published. As a result, the analysis is of limited relevance to the regulation actually proposed.

The following are examples of assumptions and costs in the analysis that do not match privacy policies or requirements stated in the proposed rule.

1. *Authorizations:* The study assumed rules requiring new authorizations from current subscribers to use their data for treatment, payment of claims, or other health plan operations. The proposed rule would have prohibited providers or plans from obtaining patient authorization to use data for treatment, payment or health care operations, and the final rule makes obtaining consent for these purposes voluntary for all health plans and for providers that do not have direct treatment relationships with individuals.

2. *Disclosure History:* The study assumes that providers, health plans, and clearinghouses would have to track all disclosures of health information. Under the NPRM and the final rule, plans, providers and clearinghouses are only required to account for disclosures that are not for treatment, payment, and health care operations, a small minority of all disclosures.

3. *Inspection, Copying, and Amendment:* The study assumed requirements to allow patients and their subscribers to inspect, copy, and amend all information that includes their name, social security number or other identifying feature (*e.g.* customer service calls, internal memorandum, claim runs). However, the study assumed broader access than provided in the rule, which requires access only to information in records used to make decisions about individuals, not all records with identifiable information.

4. *Infrastructure development:* The study attributed significant costs to infrastructure implementation of (computer systems, training, and other compliance costs). As explained below, the compliance requirements are much less extensive than assumed in this study. For example, many providers and plans will not be required to modify their privacy systems but will only be required to document their practices and notify patients of these practices, and others will be able to purchase low-cost, off-the-shelf software that will facilitate the new requirements. The final regulation will not require massive capital expenditures; we assumed, based on our consultants' work, that providers will rely on low-cost incremental adjustments initially, and as their technology becomes outdated, they will replace it with new systems that incorporate the HIPAA standard requirements.

Although many of the policy assumptions in the study are fundamentally different than those in the proposed or final regulation, the study did provide some assistance to the Department in preparing its final analysis. The Department compared data, methodologies and model assumptions, which helped us think more critically about our own analysis and enhanced the quality of our final work.

Comment: One commenter submitted a detailed analysis of the NPRM Regulatory Impact Analysis and concluded that it might cost over $64 billion over 5 years. This analysis provided an interesting framework for analyzing the provision for the rule. More precisely, the analysis generally attempted to identify the number of entities would be required to comply with each of the significant provision of the proposed rule, then estimated the numbers of hours required to comply per entity, and finally, estimated an hourly wage.

Response: HHS adopted this general structure for the final RIA because it provided a better framework for analysis than what the Department had done in the NPRM. However, HHS did not agree with many of the specific assumptions used by in this analysis, for several reasons. First, in some instances the assumptions were no longer relevant because the requirements of the NPRM were altered in the final rule. For other assumptions, HHS found more appropriate data sources for the number of covered entities, wages rates and trend rates or other factors affecting costs. In addition, HHS believes that in a few instances, this analysis over-estimated what is required of covered entities to comply. Based on public comments and its own factfinding, the Department believes many of its assumptions used in the final analysis more accurately reflect what is likely to be the real cost of the regulation.

IV. Final Regulatory Impact Analysis

5 U.S.C. 804(2) (as added by section 251 of Pub. L. 104–21), specifies that a ''major rule'' is any rule that the Office of Management and Budget finds is likely to result in:

- An annual effect on the economy of $100 million or more;
- A major increase in costs or prices for consumers, individual industries, federal, state, or local government agencies, or geographic regions; or
- Significant adverse effects in competition, employment, investment productivity, innovation, or on the ability of United States based enterprises to compete with foreign-based enterprises in domestic and export markets. The impact of this final rule will be over $1 billion in the first year of implementation. Therefore, this rule is a major rule as defined in 5 U.S.C. 804(2).

Executive Order 12866 directs agencies to assess all costs and benefits of available regulatory alternatives and, when regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects; distributive impacts; and equity). According to Executive Order 12866, a regulatory action is ''significant'' if it meets any one of a number of specified conditions, including having an annual effect on the economy of $100 million or more adversely affecting in a material way a sector of the economy, competition, or jobs, or if it raises novel legal or policy issues. The purpose of the regulatory impact analysis is to assist decision-makers in understanding the potential ramifications of a regulation as it is being developed. The analysis is also intended to assist the public in understanding the general economic ramifications of a regulation, both in the aggregate as well as the major policy areas of a regulation and how they are likely to affect the major industries or sectors of the economy covered by it.

In accordance with the Small Business Regulatory Enforcement and Fairness Act (Pub. L. 104–121), the Administrator of the Office of Information and Regulatory Affairs of the Office of Management and Budget (OMB) has determined that this rule is a major rule for the purpose of congressional review.

The proposal for the privacy regulation included a preliminary regulatory impact analysis (RIA) which estimated the cost of the rule at $3.8 billion over five years. The preliminary

analysis also noted that a number of significant areas were not included in the estimate due to inadequate information. The proposal solicited public comment on these and all other aspects of the analysis. In this preamble, the Department has summarized the public comments pertinent to the cost analysis and its response to them. However, because of the extensive policy changes incorporated in the final regulation, additional data collected from the public comments and the Department's fact-finding, and changes in the methodology underlying the estimates, the Department is setting forth in this section a more complete explanation of its revised estimates and how they were obtained. This will facilitate a better understanding by the public of how the estimates were developed and provide more insight into how the Department believes the regulation will ultimately affect the health care sector.

The impact analysis measures the effect of the regulation on current practices. In the case of privacy, as discussed in the preamble, there already exists considerable, though quite varied, efforts to protect the confidentiality of medical information. The RIA is measuring the change in these current practices and the cost of new and additional responsibilities that are required to conform to the new regulation.

To achieve a reasonable level of privacy protection, the Department defined three objectives for the final rule: (1) To establish national baseline standards, implementation specifications, and requirements for health information privacy protection, (2) to protect the privacy of individually identifiable health information maintained or transmitted by covered entities, and (3) to protect the privacy of all individually identifiable health information within covered entities, regardless of its form.

Establishing minimum standards, implementation specifications, and requirements for health information privacy protection creates a level baseline of privacy protection for patients across states. The Health Privacy Project's report, *The State of Health Privacy: An Uneven Terrain* [33] makes it clear that under the current system of state laws, privacy protection is extremely variable. The Department's statutory authority under HIPAA which allows the privacy regulation to preempt any state law if such law is contrary to and not more stringent than privacy protection pursuant to this regulation. This sets a floor, but permits a state to create laws that are more protective of privacy. We discuss preemption in greater detail in other parts of the preamble.

The second objective is to establish a uniform base of privacy protection for individually identifiable health information maintained or transmitted by covered entities. HIPAA restricts the type of entities covered by the rule to three broad categories: health care providers that transmit health information in HIPAA standard transactions, health plans, and health care clearinghouses. However, there are similar public and private entities that are not within the Department's authority to regulate under HIPAA. For example, life insurance companies are not covered by this rule but may have access to a large amount of individually identifiable health information.

The third objective is to protect the privacy of all individually identifiable health information held by covered entities, including their business associates. Health information is currently stored and transmitted in multiple forms, including electronic, paper, and oral forms. To provide consistent protection to information, and to avoid requiring covered entities from distinguishing between health information that has been transmitted or maintained electronically and that which has not, this rule covers all individually identifiable health information in any form maintained or transmitted by a covered entity.

For purposes of this cost analysis, the Department has assumed all health care providers will be affected by the rule. This results in an overestimation of costs because there are providers that do not engage in any HIPAA standard transactions, and therefore, are not affected. The Department could not obtain any reliable data on the number of such providers, but the available data suggest that there are very few such entities, and given the expected increase in all forms of electronic health care in the coming decade, the number of paper-only providers is likely to decrease.

A. Relationship of This Analysis to Analyses in Other HIPAA Regulations

Congress has recognized that privacy standards, implementation specifications and requirements must accompany the electronic data interchange standards, implementation specifications and requirements because the increased ease of transmitting and sharing individually identifiable health information will result in an increase in concern regarding privacy and confidentiality of such information. The bulk of the first Administrative Simplification section that was debated on the floor of the Senate in 1994 (as part of the Health Security Act) was made up of privacy provisions. The requirement for the issuance of concomitant privacy measures remained a part of the HIPAA bill passed by the House of Representatives in 1996, but the requirement for privacy measures was removed in conference. Instead, Congress added section 264 to Title II of HIPAA, which directs the Secretary to develop and submit to Congress recommendations addressing at least the following:

(1) The rights that an individual who is a subject of individually identifiable health information should have.

(2) The procedures that should be established for the exercise of such rights.

(3) The uses and disclosures of such information that should be authorized or required. The Secretary's Recommendations were submitted to Congress on September 11, 1997, and are summarized below. Section 264(c)(1) of HIPAA provides that: If legislation governing standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a) of the Social Security Act (as added by section 262) is not enacted by (August 21, 1999), the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than (February 21, 2000). Such regulations shall address at least the subjects described in subsection (regarding recommendations).

Because the Congress did not enact legislation governing standards with respect to the privacy of individually identifiable health information prior to August 21, 1999, the Department has, in accordance with this statutory mandate, developed final rules setting forth standards to protect the privacy of such information.

Title II of the Health Insurance Portability and Accountability Act (HIPAA) also provides a statutory framework for the promulgation of other administrative simplification regulations. On August 17, 2000, the Transactions Rule was published. Proposals for health care provider identifier (May 1998), employer identifier (June 1998), and security and electronic signature standards (August 1998) have also been published. These

[33] Janlori Goldman, Institute for Health Care Research and Policy, Georgetown University: <http://www.healthprivacy.org/resources>.

regulations are expected to be made final in the foreseeable future.

HIPAA states that, ''any standard adopted under this part shall be consistent with the objective of reducing the administrative costs of providing and paying for health care.'' (Section 1172 (b)). This provision refers to the administrative simplification regulations in their totality, including this rule regarding privacy standards. The savings and costs generated by the various standards should result in a net savings to the health care system. The Transactions Rule shows a net savings of $29.9 billion over ten years (2002–2011), or a net present value savings of $19 billion. This estimate does not include the growth in ''e-health'' and ''e-commerce'' that may be spurred by the adoption of uniform codes and standards.

This final Privacy Rule is estimated to produce net costs of $18.0 billion, with net present value costs of $11.8 billion (2003 dollars) over ten years (2003–2012). This estimate is based on some costs already having been incurred due to the requirements of the Transactions Rule, which included an estimate of a net savings to the health care system of $29.9 billion over ten years (2002 dollars) and a net present value of $19.1 billion. The Department expects that the savings and costs generated by all administrative simplification standards should result in a net savings to the health care system.

B. Summary of Costs and Benefits

Measuring both the economic costs and benefits of health information privacy is difficult. Traditionally, privacy has been addressed by state laws, contracts, and professional practices and guidelines. Moreover, these practices have been evolving as computers have dramatically increased the potential use of medical data; the scope and form of health information is likely to be very different ten years from now than it is today. This final regulation is both altering current health information privacy practice and shaping its evolution as electronic uses expand.

To estimate costs, the Department used information from published studies, trade groups and associations, public comments to the proposed regulation, and fact-finding by staff. The analysis focused on the major policy areas in the regulation that would result in significant costs. Given the vast array of institutions affected by this regulation and the considerable variation in practices, the Department sought to identify the ''typical'' current practice for each of the major policy areas and estimate the cost of change resulting from the regulation. Because of the paucity of data and incomplete information on current practices, the Department has consistently made conservative assumptions (that is, given uncertainty, we have made assumptions that, if incorrect, are more likely to overstate rather than understate the true cost).

Benefits are difficult to measure because people conceive of privacy primarily as a right, not as a commodity. Furthermore, a wide gap appears to exist between what people perceive to be the level of privacy afforded health information about them and what actually occurs with the use of such information today. Arguably, the ''cost'' of the privacy regulation is the amount necessary to bring health information privacy to these perceived levels.

The benefits of enhanced privacy protections for individually identifiable health information are significant, even though they are hard to quantify. The Department solicited comments on this issue, but no commenters offered a better alternative. Therefore, the Department is essentially reiterating the analysis it offered in the proposed Privacy Rule. The illustrative examples set forth below, using existing data on mental health, cancer screening, and HIV/AIDS patients, suggest the level of economic and health benefits that might accrue to individuals and society. Moreover, the benefits of improved privacy protection are likely to increase in the future as patients gain trust in health care practitioners' ability to maintain the confidentiality of their health information.

The estimated cost of compliance with the final rule is $17.6 billion over the ten year period, 2003–2012.[34] This includes the cost of all the major requirements for the rule, including costs to federal, state and local governments. The net present value of the final rule, applying a 11.2 percent discount rate[35], is $11.8 billion.[36]

The first year estimate is $3.2 billion (this includes expenditures that may be incurred before the effective date in 2003). This represents about 0.23 percent of projected national health expenditures for 2003.[37] By 2008, seven years after the rule's effective date, the rule is estimated to cost 0.07 percent of projected national health expenditures.

The largest cost items are the requirement to have a privacy official, $5.9 billion over ten years, and the requirement that disclosures of protected health information only involve the minimum amount necessary, $5.8 billion over ten years (see Table 1). These costs reflect the change that affected organizations will have to undertake to implement and maintain compliance with the requirements of the rule and achieve enhanced privacy of protected health information.

[34] The proposed privacy rule provided an estimate for a five-year period. However, the Transactions Rule provided a cost estimate for a ten year period. The decision was made to provide the final privacy estimates in a ten year period so that it would be possible to compare the costs and benefits of the two regulations.

[35] This based on a seven percent real discount rate, explained in OMB Circular A–94, and a projected 4.2 percent inflation rate projected over the ten-year period covered by this analysis.

[36] The regulatory impact analysis in the Transactions Rule showed a net savings of $29.9 billion (net present value of $19.1 billion in 2002 dollars). The cost estimates included all electronic systems changes that would be necessitated by the HIPAA administrative standards (*e.g.,* security, safeguards, and electronic signatures; eligibility for a health plan; and remittance advice and payment claim status), except privacy. At the time the Transactions Rule was developed, the industry provided estimates for the systems changes in the aggregate. The industry argued that affected parties would seek to make all electronic changes in one effort because that approach would be the most cost-efficient. The Department agreed, and therefore, it ''bundled'' all the system change cost in the Transactions Rule estimate. Privacy was not included because at the time the Department had not made a decision to develop a privacy rule. As the Department develops other HIPAA administrative simplification standards, there may be additional costs and savings due to the non-electronic components of those regulations, and they will be identified in regulatory impact analyses that accompany those regulations. The Department anticipates that such costs and savings will be relatively small compared to the privacy and Transactions rules. The Department anticipates that the net economic impact of the rules will be a net savings to the health care system.

[37] Health spending projections from *National Health Expenditure Projections 1998–2008* (January 2000), Health Care Financing Administration, Office of the Actuary, <*http://hcfa.hhs.gov/stats/nhe-proj/*>.

TABLE 1.—THE COST OF COMPLYING WITH THE PROPOSED PRIVACY REGULATION

[In dollars]

Provision	Initial or first year cost (2003, $million)	Average annual cost ($million, years 2–10)	Ten year cost (2003–2012) ($million)
Policy Development	597.7	0	597.7
Minimum Necessary	926.2	536.7	5,756.7
Privacy Officials	723.2	575.8	5,905.8
Disclosure Tracking/History	261.5	95.9	1,125.1
Business Associates	299.7	55.6	800.3
Notice Distribution	50.8	37.8	391.0
Consent	166.1	6.8	227.5
Inspection/Copying	1.3	1.7	16.8
Amendment	5.0	8.2	78.8
Requirements on Research	40.2	60.5	584.8
Training	287.1	50.0	737.2
De-Identification of Information	124.2	117.0	1,177.4
Employers with Insured Group Health Plans	52.4	0	52.4
Internal Complaints	6.6	10.7	103.2
Total*	3,242.0	1,556.9	17,554.7
Net Present Value	3,242.0	917.8	11,801.8

* **Note:** Numbers may not add due to rounding.

C. Need for the Final Rule

The need for a national health information privacy framework is described in detail in Section I of the preamble above. In short, privacy is a necessary foundation for delivery of high quality health care—the entire health care system is built upon the willingness of individuals to share the most intimate details of their lives with their health care providers. At the same time, there is increasing public concern about loss of privacy generally, and health privacy in particular. The growing use of interconnected electronic media for business and personal activities, our increasing ability to know an individual's genetic make-up, and the increasing complexity of the health care system each bring the potential for tremendous benefits to individuals and society, but each also brings new potential for invasions of our privacy.

Concerns about the lack of attention to information privacy in the health care industry are not merely theoretical. Section I of the preamble, above, lists numerous examples of the kinds of deliberate or accidental privacy violations that call for a national legal framework of health privacy protections. Disclosure of health information about an individual can have significant implications well beyond the physical health of that person, including the loss of a job, alienation of family and friends, the loss of health insurance, and public humiliation. The answer to these concerns is not for consumers to withdraw from the health care system, but for society to establish a clear national legal framework for privacy.

This section adds to the discussion in Section I, above, a discussion of the market failures inherent in the current system which create additional and compelling reasons to establish national health information privacy standards. Market failures will arise to the extent that privacy is less well protected than the parties would have agreed to, if they were fully informed and had the ability to monitor and enforce contracts. The chief market failures with respect to privacy of health information concern information, negotiation, and enforcement costs between the entity and the individual. The information costs arise because of the information asymmetry between the company and the patient—the company typically knows far more than the patient about how the protected health information will be used by that company. A health care provider or plan, for instance, knows many details about how protected health information may be generated, combined with other databases, or sold to third parties.

Absent this regulation, patients face at least two layers of cost in learning about how their information is used. First, as with many aspects of health care, patients face the challenge of trying to understand technical medical terminology and practices. A patient generally will have difficulty understanding medical records and the implications of transferring health information about them to a third party. Second, in the absence of consistent national rules, patients may face significant costs in trying to learn and understand the nature of a company's privacy policies.

The costs of learning about companies' policies are magnified by the difficulty patients face in detecting whether companies, in fact, are complying with those policies. Patients might try to adopt strategies for monitoring whether companies have complied with their announced policies. These sorts of strategies, however, are both costly (in time and effort) and likely to be ineffective. In addition, modern health care often requires protected health information to flow legitimately among multiple entities for purposes of treatment, payment, health care operations, and other necessary uses. Even if the patient could identify the provider whose data ultimately leaked, the patient could not easily tell which of those multiple entities had impermissibly transferred her information. Therefore, the cost and ineffectiveness of monitoring leads to less than optimal protection of individually identifiable health information.

The incentives facing a company that acquires individually identifiable health information also discourage privacy protection. A company gains the full benefit of using such information, including its own marketing efforts or its ability to sell the information to third parties. The company, however, does not suffer the losses from disclosure of protected health information; the patient does. Because of imperfect monitoring, customers often will not

learn of, and thus not be able to take efficient action to prevent uses or disclosures of sensitive information. Because the company internalizes the gains from using the information, but does not bear a significant share, if any, of the cost to patients (in terms of lost privacy), it will have a systematic incentive to over-use individually identifiable health information. In market failure terms, companies will have an incentive to use individually identifiable health information where the patient would not have freely agreed to such use.

These difficulties are exacerbated by the third-party nature of many health insurance and payment systems. Even where individuals would wish to bargain for privacy, they may lack the legal standing to do so. For instance, employers often negotiate the terms of health plans with insurers. The employee may have no voice in the privacy or other terms of the plan, facing a take-it-or-leave-it choice of whether to be covered by insurance. The current system leads to significant market failures in bargaining privacy protection. Many privacy-protective agreements that patients would wish to make, absent barriers to bargaining, will not be reached.

The economic arguments become more compelling as the medical system shifts from predominantly paper to predominantly electronic records. Rapid changes in information technology should result in increased market failures in the markets for individually identifiable health information. Improvements in computers and networking mean that the costs of gathering, analyzing, and disseminating electronic data are plunging. Market forces are leading many health care providers and health plans to shift from paper to electronic records, due both to lower cost and the increased functionality provided by having information in electronic form. These market changes will be accelerated by the administrative simplification implemented by the other regulations promulgated under HIPAA. A chief goal of administrative simplification, in fact, is to create a more efficient flow of medical information, where appropriate. This privacy regulation is an integral part of the overall effort of administrative simplification; it creates a framework for more efficient flows for certain purposes, including treatment and payment, while restricting flows in other circumstances except where appropriate institutional safeguards exist.

If the medical system shifts predominantly to electronic records in the near future, accompanying privacy rules will become more critical to prevent unanticipated, inappropriate, or unnecessary uses or disclosures of individually identifiable health information without patient consent and without effective institutional controls against further dissemination. In terms of the market failure, it will become more difficult for patients to know how their health provider or health plan is using health information about them. It will become more difficult to monitor the subsequent flows of individually identifiable health information, as the number of electronic flows and possible points of leakage both increase. Similarly, the costs and difficulties of bargaining to get the patients' desired level of use will likely rise due to the greater number and types of entities that receive protected health information.

As the benefits section, below, discusses in more detail, the protection of privacy and correcting the market failure also have practical implications. Where patients are concerned about lack of privacy protections, they might fail to get medical treatment that they would otherwise seek. This failure to get treatment may be especially likely for certain conditions, including mental health, and HIV. Similarly, patients who are concerned about lack of privacy protections may report health information inaccurately to their providers when they do seek treatment. For instance, they might decide not to mention that they are taking prescription drugs that indicate that they have an embarrassing condition. These inaccurate reports may lead to mis-diagnosis and less-than-optimal treatment, including inappropriate additional medications. In short, the lack of privacy safeguards can lead to efficiency losses in the form of forgone or inappropriate treatment.

In summarizing the economic arguments supporting the need for this regulation, the discussion here has emphasized the market failures that will be addressed by this regulation. These arguments become considerably stronger with the shift from predominantly paper to predominantly electronic records. As discussed in the benefits section below, the proposed privacy protections may prevent or reduce the risk of unfair treatment or discrimination against vulnerable categories of persons, such as those who are HIV positive, and thereby, foster better health. The proposed regulation may also help educate providers, health plans, and the general public about how protected health information is used. This education, in turn, may lead to better information practices in the future.

D. Baseline Privacy Protections

An analysis of the costs and benefits of the regulation requires a baseline from which to measure the regulation's effects. For some regulations, the baseline is relatively straightforward. For instance, an industry might widely use a particular technology, but a new regulation may require a different technology, which would not otherwise have been adopted by the industry. In this example, the old and widely used technology provides the baseline for measuring the effects of the regulation. The costs and the benefits are the difference between keeping the old technology and implementing the new technology.

Where the underlying technology and industry practices are rapidly changing, however, it can be far more difficult to determine the baseline and thereby measure the costs and benefits of a regulation. There is no simple way to know what technology industry would have chosen to introduce if the regulation had never existed, nor how industry practices would have evolved.

Today, the entities covered by the HIPAA privacy regulation are in the midst of a shift from primarily paper records to electronic records. As covered entities spend significant resources on hardware, software, and other information technology costs, questions arise about which of these costs are fairly attributable to the privacy regulations as opposed to costs that would have been expended even in the absence of the regulations. Industry practices generally are rapidly evolving, as described in more detail in Part I of this preamble. New technological or other measure taken to protect privacy are in part attributable to the expected expense of shifting to electronic medical records, rather than being solely attributable to the new regulations. In addition, the existence of privacy rules in other sectors of the economy help set a norm for what practices will be considered good practices for health information. The level of privacy protection that would exist in the health care sector, in the absence of regulations, thus would likely be affected by regulatory and related developments in other sectors. In short, it is therefore difficult to project a cost or benefits baseline for this rule.

The common security practice of using ''firewalls'' illustrates how each of the three baselines might apply. Under the first baseline, the full cost of implementing firewalls should be included in a Regulatory Impact

Analysis for a rule that expects entities to have firewalls. Because current law has not required firewalls, a new rule expecting this security measure must include the full cost of creating firewalls. This approach, however, would seem to overstate the cost of such a regulation. Firewalls would seem to be an integral part of the decision to move to an on-line, electronic system of records. Firewalls are also being widely deployed by users and industries where no binding security or privacy regulations have been proposed.

Under the second baseline, the touchstone is the level of risk of security breaches for individually identifiable health information under current practices. There is quite possibly a greater risk of breach for an electronic system of records, especially where such records are accessible globally through the Internet, than for patient records dispersed among various doctors' offices in paper form. Using the second baseline, the costs of firewalls for electronic systems should not be counted as a cost of the regulation except where firewalls create greater security than existed under the previous, paper-based system.

Finally, the third baseline would require an estimate of the typical level of firewall protections that covered entities would adopt in the absence of regulation, and include in the Regulatory Impact Analysis only the costs that exceed what would otherwise have been adopted. For this analysis, the Department has generally assumed that the status quo would otherwise exist throughout the ten-year period (in a few areas we explicitly discuss likely changes). We made this decision for two reasons. First, predicting the level of change that would otherwise occur is highly problematic. Second, it is a ''conservative'' assumption—that is, any error will likely be an overstatement of the true costs of the regulation.

Privacy practices are most often shaped by professional organizations that publish ethical codes of conduct and by state law. On occasion, state laws defer to professional conduct codes. At present, where professional organizations and states have developed only limited guidelines for privacy practices, an entity may implement privacy practices independently. However, it is worth noting that changes in privacy protection continue to increase in various areas. For example, European Union countries may only send individually identifiable information to companies, including U.S. firms, that comply with their privacy standards, and the growing use of health data in other areas of commerce, such as finance and general commercial marketing, have also increased the demand for privacy in ways that were not of concern in the past.

1. Professional Codes of Ethics

The Department examined statements issued by five major professional groups, one national electronic network association and a leading managed care association.[38] There are a number of common themes that all the organizations appear to subscribe to:

- The need to maintain and protect an individual's health information;
- The development of policies to ensure the confidentiality of individually identifiable health information;
- A restriction that only the minimum necessary information should be released to accomplish the purpose for which the information is sought.

Beyond these principles, the major associations differ with respect to the methods used to protect individually identifiable health information. There is no common professional standard across the health care field with respect to the protection of individually identifiable health information. One critical area of difference is the extent to which professional organizations should release individually identifiable health information. A major mental health association advocates the release of identifiable patient information '' * * * only when de-identified data are inadequate for the purpose at hand.'' A major association of physicians counsels members who use electronically maintained and transmitted data to require that they and their patients know in advance who has access to protected patient data, and the purposes for which the data will be used. In another document, the association advises physicians not to ''sell'' patient information to data collection companies without fully informing their patients of this practice and receiving authorization in advance to release of the information.

Only two of the five professional groups state that patients have the right to review their medical records. One group declares this as a fundamental patient right, while the second association qualifies its position by stating that the physician has the final word on whether a patient has access to his or her health information. This association also recommends that its members respond to requests for access to patient information within ten days, and recommends that entities allow for an appeal process when patients are denied access. The association further recommends that when a patient contests the accuracy of the information in his or her record and the entity refuses to accept the patient's change, the patient's statement should be included as a permanent part of the patient's record.

In addition, three of the five professional groups endorse the maintenance of audit trails that can track the history of disclosures of individually identifiable health information.

The one set of standards that we reviewed from a health network association advocated the protection of individually identifiable health information from disclosure without patient authorization and emphasized that encrypting information should be a principal means of protecting individually identifiable health information. The statements of a leading managed care association, while endorsing the general principles of privacy protection, were vague on the release of information for purposes other than treatment. The association suggested allowing the use of protected health information without the patient's authorization for what they term ''health promotion.'' It is possible that the use of protected health information for ''health promotion'' may be construed under the rule as part of marketing activities.

Based on the review of the leading association standards, we believe that the final rule embodies most or all of the major principles expressed in the standards. However, there are some major areas of difference between the rule and the professional standards reviewed. The final rule generally provides stronger, more consistent, and more comprehensive guarantees of privacy for individually identifiable health information than the professional standards. The differences between the rule and the professional codes include the individual's right of access to health information in the covered entity's possession, relationships between contractors and covered entities, and the requirement that covered entities make their privacy policies and practices available to patients through a notice

[38] American Association of Health Plans, *Code of Conduct; http:www.aahp.org.;* American Dental Association, *Principles of Ethics and Professional Conduct; http://www.ada.org.*; American Hospital Association, ''Disclosure of Medical Record Information,'' *Management Advisory: Information Management*; 1990, AHA: Chicago, IL.; American Medical Association, *AMA Policy Finder—Current Opinions Council on Ethical and Judicial Affairs*; several documents available through the Policy Finder at *http:www.ama-assn.org.*; American Psychiatric Association, ''APA Outlines Standards Needed to Protect Patient's Medical Record''; Release No. 99–32, May 27, 1999; *http:www.psych.org.*

and the ability to respond to questions related to the notice. Because the regulation requires that (with a few exceptions) patients have access to their protected health information that a covered entity possesses, large numbers of health care providers may have to modify their current practices in order to allow patient access, and to establish a review process if they deny a patient access. Also, none of the privacy protection standards reviewed require that health care providers or health plans prepare a formal statement of privacy practices for patients (although the major physician association urges members to inform patients about who would have access to their protected health information and how their health information would be used). Only one HMO association explicitly made reference to information released for legitimate research purposes. The regulation allows for the release of protected health information for research purposes without an individual's authorization, but only if the research where such authorization is waived by an institutional research board or an equivalent privacy board. This research requirement may cause some groups to revise their disclosure authorization standards.

2. State Laws

The second body of privacy protections is found in a complex, and often confusing, myriad of state laws and requirements. To determine whether or not the final rule would preempt a state law, first we identified the relevant laws, and second, we addressed whether state or federal law provides individuals with greater privacy protection.

Identifying the Relevant State Statutes: Health information privacy provisions can be found in laws applicable to many issues including insurance, worker's compensation, public health, birth and death records, adoptions, education, and welfare. In many cases, state laws were enacted to address a specific situation, such as the reporting of HIV/AIDS, or medical conditions that would impair a person's ability to drive a car. For example, Florida has over 60 laws that apply to protected health information. According to the Georgetown Privacy Project,[39] Florida is not unique. Every state has laws and regulations covering some aspect of medical information privacy. For the purpose of this analysis, we simply acknowledge the variation in state requirements.

We recognize that covered entities will need to learn the laws of their states in order to comply with such laws that are not contrary to the rule, or that are contrary to and more stringent than the rule. This analysis should be completed in the context of individual markets; therefore, we expect that professional associations or individual businesses will complete this task.

Recognizing the limits of our ability to effectively summarize state privacy laws, we discuss conclusions generated by the Georgetown University Privacy Project's report, *The State of Health Privacy: An Uneven Terrain.* The Georgetown report is among the most comprehensive examination of state health privacy laws currently published, although it is not exhaustive. The report, which was completed in July 1999, is based on a 50-state survey.

To facilitate discussion, we have organized the analysis into two sections: access to health information and disclosure of health information. Our analysis is intended to suggest areas where the final rule appears to preempt various state laws; it is not designed to be a definitive or wholly comprehensive state-by-state comparison.

Access to Subject's Information: In general, state statutes provide individuals with some access to medical records about them. However, only a few states allow individuals access to health information held by all their health care providers and health plans. In 33 states, individuals may access their hospital and health facility records. Only 13 states guarantee individuals access to their HMO records, and 16 states provide individuals access to their medical information when it is held by insurers. Seven states have no statutory right of patient access; three states and the District of Columbia have laws that only assure individuals' right to access their mental health records. Only one state permits individuals access to records about them held by health care providers, but it excludes pharmacists from the definition of provider. Thirteen states grant individuals statutory right of access to pharmacy records.

The amount that entities are allowed to charge for copying of individuals' records varies widely from state to state. A study conducted by the American Health Information Management Association [40] found considerable variation in the amounts, structure, and combination of fees for search and retrieval, and the copying of the record.

In 35 states, there are laws or regulations that set a basis for charging individuals inspecting and copying fees. Charges vary not only by state, but also by the purpose of the request and the facility holding the health information. Also, charges vary by the number of pages and whether the request is for X-rays or for standard medical information.

Of the 35 states with laws regulating inspection and copying charges, seven states either do not allow charges for retrieval of records or require that the entity provide the first copy free of charge. Some states may prohibit hospitals from charging patients a retrieval and copying fee, but allow clinics to do so. Many states allow fee structures, while eleven states specify only that the record holder may charge ''reasonable/actual costs.''

According to the report by the Georgetown Privacy Project, among states that do grant access to patient records, the most common basis for denying individuals access is concern for the life and safety of the individual or others.

The amount of time an entity is given to supply the individual with his or her record varies widely. Many states allow individuals to amend or correct inaccurate health information, especially information held by insurers. However, few states provide the right to insert a statement in the record challenging the covered entity's information when the individual and entity disagree.[41]

Disclosure of Health Information: State laws vary widely with respect to disclosure of individually identifiable health information. Generally, states have applied restrictions on the disclosure of health information either to specific entities or for specific health conditions. Only three state laws place broad limits on disclosure of individually identifiable health information without regard for policies and procedures developed by covered entities. Most states require patient authorization before an entity may disclose health information to certain recipients, but the patient often does not have an opportunity to object to any disclosures.[42]

It is also important to point out that none of the states appear to offer individuals the right to restrict disclosure of their health information for treatment.

[39] Ibid, Goldman, p. 6.

[40] ''Practice Briefs,'' Journal of AHIMA; Harry Rhodes, Joan C. Larson, Association of Health Information Outsourcing Service; January 1999.

[41] Ibid, Goldman, p. 20.

[42] Ibid, Goldman, p. 21.

State statutes often have exceptions to requiring authorization before disclosure. The most common exceptions are for purposes of treatment, payment, or auditing and quality assurance functions. Restrictions on re-disclosure of individually identifiable health information also vary widely from state to state. Some states restrict the re-disclosure of health information, and others do not. The Georgetown report cites state laws that require providers to adhere to professional codes of conduct and ethics with respect to disclosure and re-disclosure of protected health information.

Most states have adopted specific measures to provide additional protections for health information regarding certain sensitive conditions or illnesses. The conditions and illnesses most commonly afforded added privacy protection are:

- Information derived from genetic testing;
- Communicable and sexually-transmitted diseases;
- Mental health; and
- Abuse, neglect, domestic violence, and sexual assault.

Some states place restrictions on releasing condition-specific health information for research purposes, while others allow release of information for research without the patient's authorization. States frequently require that researchers studying genetic diseases, HIV/AIDS, and other sexually transmitted diseases have different authorization and privacy controls than those used for other types of research. Some states require approval from an IRB or agreements that the data will be destroyed or identifiers removed at the earliest possible time. Another approach has been for states to require researchers to obtain sensitive, identifiable information from a state public health department. One state does not allow automatic release of protected health information for research purposes without notifying the subjects that their health information may be used in research and allowing them an opportunity to object to the use of their information.[43]

Comparing state statutes to the final rule: The variability of state law regarding privacy of individually identifiable health information and the limitations of the applicability of many such laws demonstrates the need for uniformity and minimum standards for privacy protection. This regulation is designed to meet these goals while allowing stricter state laws to be enacted and remain effective. A comparison of state privacy laws with the final regulation highlights several of the rule's key implications:

- No state law requires covered entities to make their privacy and access policies available to patients. Thus, all covered entities that have direct contact with patients will be required by this rule to prepare a statement of their privacy protection and access policies. This necessarily assumes that entities have to develop procedures if they do not already have them in place.
- The rule will affect more entities than are covered or encompassed under many state laws.
- Among the three categories of covered entities, it appears that health plans will be the most significantly affected by the access provisions of the rule. Based on the Health Insurance Association of America (HIAA) data[44], there are approximately 94.7 million non-elderly persons with private health insurance in the 35 states that do not provide patients a legal right to inspect and copy their records.
- Under the rule, covered entities will have to obtain an individual's authorization before they could use or disclose their information for purposes other than treatment, payment, and health care operations—except in the situations explicitly defined as allowable disclosures without authorization. Although the final rule would establish a generally uniform disclosure and re-disclosure requirement for all covered entities, the entities that currently have the greatest ability and economic incentives to use and disclose protected health information for marketing services to both patients and health care providers without individual authorization.
- While the final rule appears to encompass many of the requirements found in current state laws, it also is clear that within state laws, there are many provisions that cover specific cases and health conditions. Certainly, in states that have no restrictions on disclosure, the rule will establish a baseline standard. But in states that do place conditions on the disclosure of protected health information, the rule may place additional requirements on covered entities.

3. Other Federal Laws

The relationship with other federal statutes is discussed above in the preamble.

E. Costs

Covered entities will be implementing the privacy final rules at the same time many of the administrative simplification standards are being implemented. As described in the overall impact analysis for the Transactions Rule, the data handling change occurring due to the other HIPAA standards will have both costs and benefits. To the extent the changes required for the privacy standards, implementation specifications, and requirements can be made concurrently with the changes required by the other regulations, costs for the combined implementation should be only marginally higher than for the administrative simplification standards alone. The extent of this incremental cost is uncertain, in the same way that the costs associated with each of the individual administrative simplification standards is uncertain.

The costs associated with implementing the requirements under this Privacy Rule will be directly related to the number of affected entities and the number of affected transactions in each entity. There are approximately 12,200 health plans (including self-insured employer and government health plans that are at least partially self-administered)[45], 6480 hospitals, and 630,000 non-hospital providers that will bear implementation costs under the final rule.

The relationship between the HIPAA security and privacy standards is particularly relevant. On August 17, 2000, the Secretary published a final rule to implement the HIPAA standards on electronic transactions. That rule adopted standards for eight electronic code sets to be used for those transactions. The proposed rule for security and electronic signature standards was published on August 12, 1998. That proposal specified the security requirements for covered entities that transmit and store information specified in Part C, Title II of the Act. In general, that proposed rule proposed administrative and technical standards for protecting ''* * * any health information pertaining to an individual that is electronically

[43] ''Medical records and privacy: Empirical effects of legislation; A memorial to Alice Hersh''; McCarthy, Douglas B; Shatin, Deborah; et al. *Health Service Research:* April 1, 1999; No. 1, Vol. 34; p. 417. The article details the effects of the Minnesota law conditioning disclosure of protected health information on patient authorization.

[44] *Source Book of Health Insurance Data: 1997–1998*, Health Insurance Association of America, 1998. p. 33.

[45] ''Health plans,'' for purposes of the regulatory impact and regulatory flexibility analyses, include licensed insurance carriers who sell health products; third party administrators that will have to comply with the regulation for the benefit of the plan sponsor; and self-insured health plans that are at least partially administered by the plan sponsor.

maintained or transmitted.'' (63 FR 43243). The final Security Rule will detail the system and administrative requirements that a covered entity must meet in order to assure itself and the Secretary that health information is safe from destruction and tampering from people without authorization for its access.

By contrast, the Privacy Rule describes the requirements that govern the circumstances under which protected health information must be used or disclosed with and without patient involvement and when a patient may have access to his or her protected health information.

While the vast majority of health care entities are privately owned and operated, we note that federal, state, and local government providers are reflected in the total costs as well. Federal, state, and locally funded hospitals represent approximately 26 percent of hospitals in the United States. This is a significant portion of hospitals, but it represents a relatively small proportion of all provider entities. We estimated that the number of government providers who are employed at locations other than government hospitals is significantly smaller (approximately two percent of all providers). Weighting the relative number of government hospital and non-hospital providers by the revenue these types of providers generate, we estimate that health care services provided directly by government entities represent 3.4 percent of total health care services. Indian Health Service and tribal facilities costs are included in the total, since the adjustments made to the original private provider data to reflect federal providers included them. In developing the rule, the Department consulted with states, representatives of the National Congress of American Indians, representatives of the National Indian Health Board, and a representative of the self-governance tribes. During the consultation we discussed issues regarding the application of Title II of HIPAA to the states and tribes.

The costs associated with this final rule involve, for each provision, consideration of both the degree to which covered entities must modify their existing records management systems and privacy policies under the final rule, and the extent to which there is a change in behavior by both patients and the covered entities as a result of the final rule. The following sections examine these provisions as they apply to the various covered entities under the final rule. The major costs that covered entities will incur are one-time costs associated with implementation of the final rules, and ongoing costs that result in continuous requirements in the final rule.

The Department has quantified the costs imposed by the final regulation to the extent possible. The cost of many provisions were estimated by first using data from the Census Bureau's Statistics of U.S. Business to identify the number of non-hospital health care providers, hospitals and health plans. Then, using the Census Bureau's Current Population Survey (CPS) wage data for the classes of employees affected by the rule, the Department identified the hourly wage of the type of employee assumed to be mostly likely responsible for compliance with a given provision. Where the Department believed a number of different types of employees might be responsible for complying with a certain provision, as is often expected to be the case, the Department established a weighted-average wage based on the types of employees involved. Finally, the Department made assumptions regarding the number of person-hours per institution required to comply with the rule.

The Department cannot determine precisely how many person-hours per institution will be required to comply with a given provision, however, the Department attempted to establish reasonable estimates based on fact-finding discussions with private sector health care providers, the advice of the Department's consultants, and the Department's own best judgement of the level of burden required to comply with a given provision. Moreover, the Department recognizes that the number of hours required to comply with a given requirement of the rule will vary from provider to provider and health plan to health plan, particularly given the flexibility and scalability permitted under the rule. Therefore, the Department considers the estimates to be averages across the entire class of health care providers, hospitals, or health plans in question.

Underlying all annual cost estimates are growth projections. For growth in the number of patients, the Department used data from the National Ambulatory Medical Care Survey, the National Hospital Ambulatory Medical Care Survey, the National Home and Hospice Survey, the National Nursing Home Survey, and information from the American Hospital Association. For growth in the number of health care workers, the Department used data from the Bureau of Health Professions in the Department's Health Resources Services Administration (HRSA). For insurance coverage growth (private and military coverage), we used a five-year average annual growth rate in employer-sponsored, individual, military, and overall coverage growth from the Census Bureau's CPS, 1995–1999. To estimate growth in the number of Medicare and Medicaid enrollees, the Department used the enrollment projections of the Health Care Financing Administration's Office of the Actuary. For growth in the number of hospitals, health care providers and health plans, trend rates were derived from the Census Bureau's Statistics of U.S. Businesses, using SIC code-specific five-year annual average growth rate from 1992–1997 (the most recent data available). For wage growth, the Department used the same assumptions made in the Medicare Trustees' Hospital Insurance Trust Fund report for 2000.

In some areas, the Department was able to obtain very reliable data, such as survey data from the Statistics of U.S. Businesses and the Medical Expenditures Panel Survey (MEPS). In numerous areas, however, there was too little information or data to support quantitative estimates. As a result, the Department relied on data provided in the public comments or subsequent fact-finding to provide a basis for making key assumptions. We were able to provide a reasonable cost estimate for virtually all aspects of the regulation, except law enforcement. In this latter area, the Department was unable to obtain sufficient data about current practices (*e.g.,* the number of criminal and civil investigations that may involve requests for protected health information, the number of subpoenas for protected health information, etc.) to determine the marginal effects of the regulation. As discussed more fully below, the Department believes the effects of the final rule are marginal because the policies adopted in the final rule appear to largely reflect current practice.

The NPRM included an estimate of $3.8 billion for the privacy proposal. The estimate for the final rule is $18.0 billion. Much of the difference can be explained by two factors. First, the NPRM estimate was for five years; the final rule estimate is for ten years. The Department chose the longer period for the final rule because ten years was also the period of analysis in the Transactions Rule RIA, and we wanted to facilitate comparisons, given that the net benefits and costs of the administrative simplification rules should be considered together. Second, the final impact analysis includes cost estimates for a number of key provisions that were not estimated in the NPRM because the Department did not have adequate information at the time.

Although we received little useable data in the public comments (see comment and response section), the Department was able to undertake more extensive fact-finding and collect sufficient information to make informed assumptions about the level of effort and time various provisions of the final rule are likely to impose on different types of affected entities.

The estimate of $18.0 billion represents a gross cost, not a net cost. As discussed more fully below in the benefits section, the benefits of enhanced privacy and confidentiality of personal health information are very significant. If people believe their information will be used properly and not disseminated beyond certain bounds without their knowledge and consent, they will be much more likely to seek proper health care, provide all relevant health information, and abide by their providers' recommendations. In addition, more confidence by individuals and covered entities that privacy will be maintained will lead to an increase in electronic transactions and the efficiencies and cost savings that stem from such action. The benefits section quantifies some examples of benefits. The Department was not able to identify data sources or models that would permit us to measure benefits more broadly or accurately. The inability to quantify benefits, however, does not lessen the importance or value that is ultimately realized by having a national standard for health information privacy.

The largest initial costs resulting from the final Privacy Rule stem primarily from the requirement that covered entities use and disclose only the minimum necessary protected health information, that covered entities develop policies and codify their privacy procedures, and that covered entities designate a privacy official and train all personnel with access to individually identifiable health information. The largest ongoing costs will result from the minimum necessary provisions pertaining internal uses of individually identifiable health information, and the cost of a privacy official. In addition, covered entities will have recurring costs for training, disclosure tracking and notice requirements. A smaller number of large entities may have significant costs for de-identification of protected health information and additional requirements for research.

The privacy costs are in addition to the Transactions Rule estimates. The cost of complying with the regulation represents approximately 0.23 percent of projected national health expenditures the first year the regulation is enacted. The costs for the first eight years of the final regulation represents 0.07 percent of the increase in national health care costs experienced over the same period.[46]

Minimum Necessary

The ''minimum necessary'' policy in the final rule has essentially three components: first, it does not pertain to certain uses and disclosures including treatment-related exchange of information among health care providers; second, for disclosures that are made on a routine and recurring basis, such as insurance claims, a covered entity is required to have policies and procedures for governing such exchanges (but the rule does not require a case-by-case determination); and third, providers must have a process for reviewing non-routine requests on a case-by-case basis to assure that only the minimum necessary information is disclosed.

Based on public comments and subsequent fact-finding, the Department has concluded that the requirements of the final rule are generally similar to the current practice of most providers. For standard disclosure requests, for example, providers generally have established procedures for determining how much health information is released. For non-routine disclosures, providers have indicated that they currently ask questions to discern how much health information is necessary for such disclosure. Under the final rule, we anticipate providers will have to be more thorough in their policies and procedures and more vigilant in their oversight of them; hence, the costs of this provision are significant.

To make the final estimates for this provision, the Department considered the minimum necessary requirement in two parts. First, providers, hospitals, and health plans will need to establish policies and procedures which govern uses and disclosures of protected health information. Next, these entities will need to adjust current practices that do not comply with the rule, such as updating passwords and making revisions to software.

To determine the policies and procedures for the minimum necessary requirement, the Department assumed that each hospital would spend 160 hours, health plans would spend 107 hours, and non-hospital providers would spend 8 hours. As noted above, the time estimates for this and other provisions of the rule are considered an average number of person-hours for the institutions involved. An underlying assumption is that some hospitals, and to a lesser extent health plans, are part of chains or larger entities that will be able to prepare the basic materials at a corporate level for a number of covered entities.

Once the policies and procedures are established, the Department estimates there will be costs resulting from implementing the new policies and procedures to restrict internal uses of protected health information to the minimum necessary. Initially, this will require 560 hours for hospitals, 160 hours for health plans, and 12 hours for non-hospital providers.[47] The wage for health care providers and hospitals is estimated at $47.28, a weighted average of various health care professionals based on CPS data; the wage for health plans is estimated to be $33.82, based on average wages in the insurance industry (note that all wage assumptions in this impact analysis assume a 39 percent load for benefits, the standard Bureau of Labor Statistics assumption). In addition, there will be time required on an annual basis to ensure that the implemented practices continue to meet the requirements of the rule. Therefore, the Department estimates that on an annual ongoing basis (after the first year), hospitals will require 320 hours, health plans 100 hours, and non-hospital providers 8 hours to comply with this provision.

The initial cost attributable to the minimum necessary provision is $926 million. The total cost of the provision is $5.757 billion. (These estimates are for the cost of complying with the minimum necessary provisions that restrict internal uses to the minimum necessary. The Department has estimated in the business associates section below the requirement limiting disclosures outside the covered entity to the minimum amount necessary.)

Privacy Official

The final rule requires entities to designate a privacy official who will be responsible for the development and implementation of privacy policies and procedures. In this cost analysis, the Department has estimated each of the primary administrative requirements of the rule (e.g., training, policy and

[46] Health Care Finance Administration, Office of the Actuary, 2000. Estimates for the national health care expenditure accounts are only available through 2008; hence, we are only able to make the comparison through that year.

[47] These estimates were, in part, derived from a report prepared for the Department by the Gartner Group, consultants in health care information technology: ''Gartner DHHS Privacy Regulation Study,'' by Jim Klein and Wes Rishel, submitted to the Office of the Assistant Secretary for Policy and Evaluation on October 20, 2000.

procedure development, etc), including the development and implementation costs associated with each specific requirement. These activities will certainly involve the privacy official to some degree; thus, some costs for the privacy official, particularly in the initial years, are subsumed in other cost requirements. Nonetheless, we anticipate that there will be additional ongoing responsibilities that the privacy official will have to address, such as coordinating between departments, evaluating procedures and assuring compliance. To avoid double-counting, the cost calculated in this section is only for the ongoing, operational functions of a privacy official (e.g., clarifying procedures for staff) that are in addition to items discussed in other sections of this impact analysis.

The Department assumes the privacy official role will be an additional responsibility given to an existing employee in the covered entity, such as an office manager in a small entity or a compliance official in a larger institution. Moreover, today any covered entity that handles individually identifiable health information has one or more people with responsibility for handling and protecting the confidentiality of such information. As a result of the specific requirement for a privacy official, the Department assumes covered entities will centralize this function, but the overall effort is not likely to increase significantly. Specifically, the Department has assumed non-hospital providers will need to devote, on average, an additional 30 minutes per week of an official's time (i.e., 26 hours per year) to compliance with the final regulation for the first two years and 15 minutes per week for the remaining eight years (i.e., 13 hours per year). For hospitals and health plans, which are more likely to have a greater diversity of activities involving privacy issues, we have assumed three hours per week for the first two years (i.e., 156 hours per year), and 1.5 hours per week for the remaining eight years (i.e., 78 hours per year).

For non-hospital providers, the time was calculated at a wage of $34.13 per hour, which is the average wage for managers of medicine and health according to the CPS. For hospitals, we used a wage of $79.44, which is the rate for senior planning officers.[48] For health plans, the Department assumed a wage of $88.42 based on the wage for top claims executives.[49] Although individual hospitals and health plans may not necessarily select their planning officers or claims executives to be their privacy officials, we believe they will be of comparable responsibility, and therefore comparable pay, in larger institutions.

The initial year cost for privacy officials will be $723 million; the ten-year cost will be $5.9 billion.

Internal Complaints

The final rule requires each covered entity to have an internal process to allow an individual to file a complaint concerning the covered entity's compliance with its privacy policies and procedures. The requirement includes designating a contact person or office responsible for receiving complaints and documenting the disposition of them, if any. This function may be performed by the privacy official, but because it is a distinct right under the final rule and may be performed by someone else, we are costing it separately.

The covered entity only is required to receive and document a complaint (no response is required), which we assume will take, on average, ten minutes (the complaint can be oral or in writing). The Department believes that such complaints will be uncommon. We have assumed that one in every thousand patients will file a complaint, which is approximately 10.6 million complaints over ten years. Based on a weighted-average hourly wage of $47.28 at ten minutes per complaint, the cost of this policy is $6.6 million in the first year. Using wage growth and patient growth assumptions, the cost of this policy is $103 million over ten years.

Disclosure Tracking and History

The final rule requires providers to be able to produce a record of all disclosures of protected health information, except in certain circumstances. The exceptions include disclosures for treatment, payment, health care operations, or disclosures to an individual. This requirement will require a notation in the record (electronic or paper) of when, to whom, and what information was disclosed, as well as the purpose of such disclosure or a copy of an individual's written authorization or request for a disclosure.

Based on information from several hospital sources, the Department assumes that all hospitals already track disclosures of individually identifiable health information and that 15 percent of all patient records held by a hospital will have an annual disclosure that will have to be recorded in an individual's record. It was more difficult to obtain a reliable estimate for non-hospital providers, though it appears that they receive many fewer requests. The Department assumed a ten percent rate for ambulatory care patients and five percent, for nursing homes, home health, dental and pharmacy providers. (It was difficult to obtain any reliable data for these latter groups, but those we talked to said that they had very few, and some indicated that they currently keep track of them in the records.) These estimated percentages represent about 63 million disclosures that will have to be recorded in the first year, with each recording estimated to require two minutes. At the average nurse's salary of $30.39 per hour, the cost in the first year is $25.7 million. For health plans, the Department assumed that disclosures of protected health information are more rare than for health care providers. Therefore, the Department assumed that there will be disclosures of protected health information for five percent of covered lives. At the average wage for the insurance industry of $33.82 per hour, the initial cost for health plans is $6.8 million. Using our standard growth rates for wages, patients, and covered entities, the ten-year cost for providers and health plans is $519 million.

In addition, although hospitals generally track patient disclosures today, the Department assumes that hospitals will seek to update software systems to assure full compliance. Based on software upgrade costs provided by the Department's private sector consultants with expertise in the area (the Gartner Group), the Department assumed that each upgrade would cost $35,000 initially and $6,300 annually thereafter, for a total cost of $572 million over ten years.

The final rule also requires covered entities to provide individuals with an accounting of disclosures upon request. The Department assumes that few patients will request a history of disclosures of their protected medical information. Therefore, we estimate that one in a thousand patients will request such an accounting each year, which is approximately 850,000 requests. If it takes an average of five minutes to copy any disclosures and the work is done by a nurse, the cost for the first year will be $2.1 million. The total ten-year cost is $33.8 million.

[48] ''Top Compensation in the Healthcare Industry, 1997'', Coopers & Lybrand, New York, NY., <http://www.pohly.com/salary/2.shtml>.

[49] ''A Unifif Survey of Compensation in Financial Services: 2000,'' July 2000, Unifi Network Survey unit, PriceWaterhouseCoopers LLP and Global HR Solutions LLC, Westport, Ct., <http://public.wsj.com/careers/resources/documents/20000912-insuranceexecs-tab.htm>.

De-Identification of Information

The rule allows covered entities to determine that health information is de-identified (i.e., that it is not individually identifiable health information) if certain conditions are met. Currently, some entities release de-identified information for research purposes. De-identified information may originate from automated systems (such as records maintained by pharmacy benefit managers) and non-automated systems (such as individual medical records maintained by providers). As compared with current practice, the rule requires that an expanded list of identifiers be removed for the data (such as driver's license numbers, and detailed geographic and certain age information). For example, as noted in a number of public comments, currently complete birth dates (day, month, and year) and zip codes are often included in de-identified information. The final rule requires that only the year of birth (except in certain circumstances) and the first three digits of the zip code can be included in de-identified information.

These changes will not require extensive change from current practice. Providers generally remove most of the 19 identifiers listed in the final rule. The Department relied on Gartner Group estimates that some additional programmer time will be required by covered entities that produce de-identified information to make revisions in their procedures to eliminate additional identifiers. Entities that de-identify information will have to review existing and future data flows to assure compliance with the final rule. For example, an automated system may need to be re-programmed to remove additional identifiers from otherwise protected health information. (The costs of educating staff about the de-identification requirements are included in the cost estimate for training staff on privacy policies.)

The Department was not able to obtain any reliable information on the volume of medical data that is currently de-identified. To provide some measure of the potential magnitude, we assumed that health plans and hospitals would have an average of two existing agreements that would need to be reviewed and modified. Based on information provided by our consultants, we estimate that these agreements would require an average of 152 hours by hospitals and 116 hours by health plans to review and revise existing agreements to conform to the final rule. Using the weighted average wage of $47.28, the initial costs will be $124 million. Using our standard growth rates for wages, patients, and covered entities, the total cost of the provision is $1.1 billion over ten years.

The Department expects that the final rule and the increasing trend toward computerization of large record sets will result over time in de-identification being performed by relatively few firms or associations. Whether the covered entity is a small provider with relatively few files or a hospital or health plan with large record files, it will be more efficient to contract with specialists in these firms or associations (as ''business associates'' of the covered entity) to de-identify files. The process will be different but the ultimate cost is likely to be the same or only slightly higher, if at all, than the costs for de-identification today. The estimate is for the costs required to conform existing and future agreements to the provisions of the rule. The Department has not quantified the benefits that might arise from changes in the market for de-identified information because the centralization and efficiency that will come from it will not be fully realized for several years, and we do not have a reliable means of estimating such changes.

Policy and Procedures Development

The final regulation imposes a variety of requirements which collectively will necessitate entities to develop policies and procedures (henceforth in this section to be referred to as policies) to establish and maintain compliance with the regulation. These include policies such as those for inspection and copying, amending records, and receiving complaints.[50] In developing the final regulations, simplifying the administrative burden was a significant consideration. To the extent practical, consistent with maintaining adequate protection of protected health information, the final rule is designed to encourage the development of policies by professional associations and others, that will reduce costs and facilitate greater consistency across providers and other covered entities.

The development of policies will occur at two levels: first, at the association or other large scale levels; and second, at the entity level. Because of the generic nature of many of the final rule's provisions, the Department anticipates that trade, professional associations, and other groups serving large numbers of members or clients will develop materials that can be used broadly. These will likely include the model privacy practice notice that all covered entities will have to provide patients; general descriptions of the regulation's requirements appropriate for various types of health care providers; checklists of steps entities will have to take to comply; training materials; and recommended procedures or guidelines. The Department spoke with a number of professional associations, and they confirmed that they would expect to provide such materials for their members at either the federal or state level.

Using Faulkner and Gray's *Health Data Directory 2000*, we identified 216 associations that would be likely to provide guidance to members. In addition, we assume three organizations (i.e., one for hospitals, health plans, and other health care providers) in each state would also provide some additional services to help covered entities coordinate the requirements of this rule with state laws and requirements. The Department assumed that these associations would each provide 320 hours of legal analysis at $150 per hour, and 640 hours of senior analysts time at $50 per hour. This equals $17.3 million. Hourly rates for legal council are the average billing rate for a staff attorney.[51] The senior analysts rates are based on a salary of $75,000 per year, plus benefits, which was provided by a major professional association.

For larger health care entities such as hospitals and health plans, the Department assumed that the complexity of their operations would require them to seek more customized assistance from outside council or consultants. Therefore, the Department assumes that each hospital and health plan (including self-administered, self-insured health plans) will, on average, require 40 hours of outside assistance. The resulting cost for external policy development is estimated to be $112 million.

All covered entities are expected to require some time for internal policy development beyond what is provided by associations or outside consultants. For most non-hospital providers, the external assistance will provide most of the necessary information. Therefore, we expect these health care providers will need only eight hours to adapt these policies for their specific use (training cost is estimated separately in the impact analysis). Hospitals and

[50] The cost for policies for minimum necessary, because they will be distinct and extensive, are presented separately, above.

[51] ''The Altman Weil 1999 Survey of Law Firm Economics,'' <*http://www.altmanweil.com/publications/survey/sife99/standard.htm*>.

health plans, which employ more individuals and are involved in a wider array of endeavors, are likely to require more specific policies tailored to their operations to comply with the final rule. For these entities, we assume an average of 320 hours of policy development per institution. The total cost for internal policy development is estimated to be $468 million.

The total cost for policy, plan, and procedures development for the final regulation is estimated to be $598 million. All of these costs are initial costs.

Training

The final regulation's requirements provide covered entities with considerable flexibility in how to best fulfill the necessary training of their workforce. As a result, the actual practices may vary substantially based on such factors as the number of members of the workforce, the types of operations, worker turnover, and experience of the workforce. Training is estimated to cost $737 million over ten years. The Department estimates that at the time of the effective date, approximately 6.7 million health care workers will have to be trained, and in the subsequent ten years, 7 million more will have to be trained because of worker turnover. The estimate of employee numbers are based on 2000 CPS data regarding the number of health care workers who indicated they worked for a health care institution. To estimate a workforce turnover rate, the Department relied on a study submitted in the public comments which used a turnover rate of ten percent or less, depending on the labor category. To be conservative, the Department assumed ten percent for all categories.

Covered entities will need to provide members of the workforce with varying amounts of training depending on their responsibilities, but on average, the Department estimates that each member of the workforce who is likely to have access to protected health information will require one hour of training in the policies and procedures of the covered entity. The initial training cost estimate is based on teacher training with an average class size of ten. After the initial training, the Department expects some training (for example, new employees in larger institutions) will be done by videotape, video conference, or computer, all of which are likely to be less expensive. Training materials were assumed to cost an average of $2 per worker. The opportunity cost for the training time is based on the average wage for each health care labor category listed in the CPS, plus a 39 percent load for benefits. Wages were increased based on the wage inflation factor utilized for the short-term assumptions (which covers ten years) in the Medicare Trustees' Annual Report for 1999.

Notice

This section describes only the cost associated with the production and provision of a notice. The cost of developing the policy stated in the notice is covered under policies and procedures, above.

Covered health care providers with direct treatment relationships are required to provide a notice of privacy practices no later than the date of the first service delivery to individuals after the compliance date for the covered health care provider. The Department assumed that for most types of health care providers (such as physicians, dentists, and pharmacists) one notice would be distributed to each patient during his or her first visit following the compliance date for the covered provider, but not for subsequent visits. For hospitals, however, the Department assumed that a notice would be provided at each admission, regardless of how many visits an individual has in a given year. In subsequent years, the Department assumed that non-hospital providers would only provide notices to their new patients, because it is assumed that providers can distinguish between new and old patients, although hospitals will continue to provide a notice for each admission. The total number of notices provided in the initial year is estimated to be 816 million.

Under the final rule, only providers that have direct treatment relationships with individuals are required to provide notices to them. To estimate the number of visits that trigger a notice in the initial year and in subsequent years, the Department relied on the Medical Expenditure Panel Survey (MEPS, 1996 data) conducted by the Department's Agency for Healthcare Quality and Research. This data set provides estimates for the number of total visits to a variety of health care providers in a given year and estimates of the number of patients with at least one visit to each type of each care provider. To estimate the number of new patients in a given year, the Department used the National Ambulatory Medical Care Survey and the National Hospital Ambulatory Medical Care Survey, which indicate that for ambulatory care visits to physician offices and hospital ambulatory care departments, 13 percent of all patients are new. This data was used as a proxy for other types of providers, such as dentists and nursing homes, because the Department did not have estimates for new patients for other types of providers. The number of new patients was increased over time to account for growth in the patient population. Therefore, the number of notices provided in years 2004 through 2012 is estimated to be 5.3 billion.

For health plans, the Department estimated the number of notices by trending forward the average annual rate of growth from 1995 through 1998 (the most recent data available) of private policy holders using the Census Bureau's Current Population Survey, and also by using Health Care Financing Administration Office of the Actuary's estimates for growth in Medicare and Medicaid enrollment. It should be noted that the regulation does not require that the notice be mailed to individuals. Therefore, the Department assumed that health plans would include their privacy policy in the annual mailings they make to members, such as by adding a page to an existing information booklet.

Since clinical laboratories generally do not have direct contact with patients, they would not normally be required to provide notices. However, there are some laboratory services that involve direct patient contact, such as patients who have tests performed in a laboratory or at a health fair. We found no data from which we could estimate the number of such visits. Therefore, we have assumed that labs would incur no costs as a result of this requirement.

The printing cost of the policy is estimated to be $0.05, based on data obtained from the Social Security Administration, which does a significant number of printings for distribution. Some large bulk users, such as health plans, can probably reproduce the document for less, and small providers simply may copy the notice, which would also be less than $0.05. Nonetheless, at $0.05, the total cost of the initial notice is $50.8 million.

Using our standard growth rate for patients, the total cost for notices is estimated to be $391 million for the ten-year period.

Requirements on Use and Disclosure for Research

The final regulation places certain requirements on covered entities that supply individually identifiable health information to researchers. As a result of these requirements, researchers who seek such health information and the Institutional Review Boards (IRBs) that review research projects will have additional responsibilities. Moreover, a covered entity doing research, or another entity requesting disclosure of

protected health information for research that is not currently subject to IRB review (research that is 100 percent privately funded and which takes place in institutions which do not have ''multiple project assurances'') may need to seek IRB or privacy board approval if they want to avoid the requirement to obtain authorization for use or disclosure of protected health information for research, thereby creating the need for additional IRBs and privacy boards that do not currently exist.

To estimate the additional requirements placed on existing IRBs, the Department relied on a survey of IRBs conducted by James Bell Associates on behalf of NIH and on estimates of the total number of existing IRBs provided by NIH staff. Based on this information, the Department concluded that of the estimated 4,000 IRBs in existence, the median number of initial current research project reviews is 133 per IRB, of which only ten percent do not receive direct consent for the use of protected health information. (Obtaining consent nullifies the need for IRB privacy scrutiny.) Therefore, in the first year of implementation, there will be 76,609 initial reviews affected by the regulation, and the Department assumes that the requirement to consider the privacy protections in the research protocols under review will add an average of 1 hour to each review. The cost to researchers for having to develop protocols which protect protected health information is difficult to estimate, but the Department assumes that each of the affected 76,609 studies will require an average of an additional 8 hours of time for protocol development and implementation. At the average medical scientist hourly wage of $46.61, the initial cost is $32.1 million; the total ten-year cost of these requirements is $468 million over ten years.

As stated above, some privately funded research not subject to any IRB review currently may need to obtain IRB or privacy board approval under the final rule. Estimating how much research exists which does not currently go through any IRB review is highly speculative, because the experts consulted by the Department all agree that there is no data on the volume of privately funded research. Likewise, public comments on this subject provided no useful data. However, the Department assumed that most research that takes place today is subject to IRB review, given that so much research has some government funding and many large research institutions have multiple project assurances. As a result, the Department assumed that the total volume of non-IRB reviewed research is equal to 25 percent of all IRB-reviewed research, leading to 19,152 new IRB or privacy board reviews in the first year of the regulation. Using the same assumptions as used above for wages, time spent developing privacy protection protocols for researchers, and time spent by IRB and privacy board members, the total one-year cost for new IRB and privacy board reviews is $8 million.

For estimating total ten-year costs, the Department used the Bell study, which showed an average annual growth rate of 3.7 percent in the number of studies reviewed by IRBs. Using this growth rate, the total ten-year cost for the new research requirements is $117 million.

Consent

Under the final rule, a covered health care provider with direct treatment relationships must obtain an individual's consent for use or disclosure of protected health information for treatment, payment, or health care operations. Covered providers with indirect treatment relationships and health plans may obtain such consent if they so choose. Providers and health plans that seek consent under this rule can condition treatment or enrollment upon provision of such consent. Based on public comments and discussions with a wide array of health care providers, it is apparent that most currently obtain written consent for use and disclosure of individually identifiable health information for payment. Under the final rule, they will have to obtain consent for treatment and health care operations, as well, but this may entail only minor changes in the language of the consent to incorporate these other categories and to conform to the rule.

Although the Department was unable to obtain any systematic data, the anecdotal evidence suggests that most non-hospital providers and virtually all hospitals follow this practice. For the cost analysis, the Department assumes that 90 percent of the non-hospital providers and all hospitals currently obtain some consent for use and disclosure of individually identifiable health information. For providers that currently obtain written consent, there is only a nominal cost for changing the language on the document to conform to the rule. For this activity, we assumed $0.05 cost per document for revising existing consent documents.

For the ten percent of treating providers who currently do not obtain consent, there is the cost of creating consent documents (which will be standardized), which is also assumed to be $0.05 per document. It is assumed that all providers required to obtain consent under the rule will do so upon the first visit, so there will be no mailing cost. For non-hospital providers, we assume the consent will be maintained in paper form, which is what most providers currently do (electronic form, if available, is cheaper to maintain). There is no new cost for records maintenance because the consent will be kept in active files (paper or electronic).

The initial cost of the consent requirement is estimated to be $166 million. Using our standard assumptions for patient growth, the total costs for the ten years is estimated to be $227 million.

Authorizations

Patient authorizations are required for uses or disclosures of protected health information that are not otherwise explicitly permitted under the final rule with or without consent. In addition to uses and disclosures of protected health information for treatment, payment, and health care operations with or without consent, the rule also permits certain uses of protected health information, such as fund-raising for the covered entity and certain types of marketing activity, without prior consent or authorization. Authorizations are generally required if a covered entity wants to provide protected health information to third party for use by the third party for marketing or for research that is not approved by an IRB or privacy board.

The requirement for obtaining authorizations for use or disclosure of protected health information for most marketing activity will make direct third-party marketing more difficult because covered entities may not want to obtain and track such authorizations, or they may obtain too few to make the effort economically worthwhile. However, the final rule permits an alternative arrangement: the covered entity can engage in health-related marketing on behalf of a third party, presumably for a fee. Moreover, the covered entity could retain another party, through a business associate relationship, to conduct the actual health-related marketing, such as mailings or telemarketing, under the covered entity's name. The Department is unable to estimate the cost of these changes because there is no credible data on the extent of current third party marketing practices or the price that third party marketers currently pay for information from covered entities. The effect of the final rule is to change the

arrangement of practices to enhance accountability of protected health information by the covered entity and its business associates; however, there is nothing inherently costly in these changes.

Examples of other circumstances in which authorizations are required under the final rule include disclosure of protected health information to an employer for an employment physical, pre-enrollment underwriting for insurance, or the sharing of protected health insurance information by an insurer with an employer. The Department assumes there is no new cost associated with these requirements because providers have said that obtaining authorization under such circumstances is current practice.

To use or disclose psychotherapy notes for most purposes (including for treatment, payment, or health care operations), a covered entity must obtain specific authorization by the individual that is distinct from any authorization for use and disclosure of other protected health information. This is current practice, so there is no new cost associated with this provision.

Confidential Communications

The final rule permits individuals to receive communications of protected health information from a covered health care provider or a health plan by an alternative means or at an alternative address. A covered provider and a health plan must accommodate reasonable requests; however, a health plan may require the individual to state that disclosure of such information may endanger the individual. A number of providers and health plans indicated that they currently provide this service for patients who request it. For providers and health plans with electronic records system, maintaining separate addresses for certain information is simple and inexpensive, requiring little or no change in the system. For providers with paper records, the cost may be higher because they will have to manually check records to determine which information must be treated in accordance with such requests. Although some providers currently provide this service, the Department was unable to obtain any reliable estimate of the number of such requests today or the number of providers who perform this service. The cost attributable to this requirement to send materials to alternate addresses does not appear to be significant.

Employers With Insured Group Health Plans

Some group health plans will use or maintain protected health information, particularly group health plans that are self-insured. Also, some plan sponsors that perform administrative functions on behalf of their group health plans, may need protected health information. The final rule permits a group health plan, or a health insurance issuer or HMO that provides benefits on behalf of the group health plan, to disclose protected health information to a plan sponsor who performs administrative functions on its behalf for certain purposes and if certain requirements are met. The plan documents must be amended to: describe the permitted uses and disclosures of protected health information by the plan sponsor; specify that disclosure is permitted only upon receipt of a certification by the plan sponsor that the plan documents have been amended and the plan sponsor agrees to certain restrictions on the use of protected health information; and provide for adequate firewalls to assure unauthorized personnel do not have access to individually identifiable health information.

Some plan sponsors may need information, not to administer the group health plan, but to amend, modify, or terminate the plan. ERISA case law describes such activities as settlor functions. For example, a plan sponsor may want to change its contract from a preferred provider organization to a health maintenance organization (HMO). In order to obtain premium information, the plan sponsor may need to provide the HMO with aggregate claims information. Under the rule, the plan sponsor can obtain summary information with certain identifiers removed, in order to provide it to the HMO and receive a premium rate.

The Department assumes that most plan sponsors who are small employers (those with 50 or fewer employees) will elect not to receive protected health information because they will have little, if any, need for such data. Any needs that plan sponsors of small group health plans may have for information can be accomplished by receiving the information in summary form. The Department has assumed that only 5 percent of plan sponsors of small group health plans that provide coverage through a contract with an issuer will actually take the steps necessary to receive protected health information. This is approximately 96,900 firms. For these firms, the Department assumes it will take one hour to determine procedural and organization issues and an additional ⅓ hour of an attorney's time to make plan document changes, which will be simple and essentially standardized. This will cost $7.1 million.

Plan sponsors who are employers of medium (51–199 employees) and large (over 200 employees) firms that provide health benefits through contracts with issuers are more likely to want access to protected health information for plan administration, for example to use it to audit claims or perform quality assurance functions on behalf of the group health plan. The Department assumes that 25 percent of plan sponsors of medium sized firms and 75 percent of larger firms will want to receive protected health information. This is approximately 38,000 medium size firms and 27,000 larger firms. To provide access to protected health information by the group health plan, a plan sponsor will have to assess the current flow of protected health information from their issuer and determine what information is necessary and appropriate. The plan sponsors may then have to make internal organizational changes to assure adequate protection of protected health information so that the relevant requirements are met for the group health plan. We assume that medium size firms will take 16 work hours to complete organizational changes, plus one hour of legal time to make changes to plan documents and certify to the insurance carrier that the firm is eligible to receive protected health information. We assume that larger firms will require 32 hours of internal organizational work and one hour of legal time. This will cost $52.4 million and is a one-time expense.

Business Associates

The final rule requires a covered entity to have a written contract or other arrangement that documents satisfactory assurance that business associate will appropriately safeguard protected health information in order to disclose it to a business associate based on such an arrangement. The Department expects business associate contracts to be fairly standardized, except for language that will have to be tailored to the specific arrangement between the parties, such as the allowable uses and disclosures of information. The Department assumes the standard language initially will be developed by trade and professional associations for their members. Small providers are likely to simply adopt the language or make minor modifications, while health plans and hospitals may start with the prototype language but may make more specific changes to

meet their institutional needs. The regulation includes a requirement that the covered entity take steps to correct, and in some cases terminate, a contract, if necessary, if they know of violations by a business associate. This oversight requirement is consistent with standard oversight of a contract.

The Department could not derive a per entity cost for this work directly. In lieu of this, we have assumed that the trade and professional associations' work plus any minor tailoring of it by a covered entity would amount to one hour per non-hospital provider and two hours for hospitals and health plans. The larger figure for hospitals and health plans reflects the fact that they are likely to have a more extensive array of relationships with business associates.

The cost for the changes in business associate contracts is estimated to be $103 million. This will be an initial year cost only because the Department assumes that this contract language will become standard in future contracts.

In addition, the Department has estimated the cost for business associates to comply with the minimum necessary provisions. As part of the minimum necessary provisions, covered entities will have to establish policies to ensure that only the minimum necessary protected health information is shared with business associates. To the extent that data are exchanged, covered entities will have to review the data and systems programs to assure compliance.

For non-hospital providers, we estimate that the first year will require an average of three hours to review existing agreements, and thereafter, they will require an additional hour to assure business associate compliance. We estimate that hospitals will require an additional 200 hours the first year and 16 hours in subsequent years; health plans will require an additional 112 hours the first year and 8 hours in subsequent years. As in other areas, we have assumed a weighted average wage for the respective sectors.

The cost of the covered entities assuring business associates' complying with the minimum necessary is $197 million in the first year, and a total of $697 million over ten years. (These estimates include the both the cost for the covered entity and the business associates.)

Inspection and Copying

In the NPRM estimate, inspection and copying were a major cost. Based on data and information from the public comments and further fact-finding, however, the Department has re-estimated these policies and found them to be much less expensive.

The public comments demonstrate that copying of records is wide-spread today. Records are routinely copied, in whole or in part, as part of treatment or when patients change providers. In addition, copying occurs as part of legal proceedings. The amount of inspection and copying of medical records that occurs for these purposes is not expected to change measurably as a result of the final regulation.

The final regulation establishes the right of individuals to access, that is to inspect and obtain a copy of, protected health information about them in designated record sets. Although this is an important right, the Department does not expect it to result in dramatic increases in requests from individuals. The Georgetown report on state privacy laws indicates that 33 states currently give patients some right to access medical information. The most common right of access granted by state law is the right to inspect personal information held by physicians and hospitals. In the process of developing estimates for the cost of providing access, we assumed that most providers currently have procedures for allowing patients to inspect and obtain a copy of individually identifiable health information about themselves. The economic impact of requiring entities to allow individuals to access their records should be relatively small. One public commenter addressed this issue and provided specific data which supports this conclusion.

Few studies address the cost of providing medical records to patients. The most recent was a study in 1998 by the Tennessee Comptroller of the Treasury. It found an average cost of $9.96 per request, with an average of 31 pages per request. The cost per page of providing copies was $0.32 per page. This study was performed on hospitals only. The cost per request may be lower for other types of providers, since those seeking hospital records are more likely to have more complicated records than those in a primary care or other types of offices. An earlier report showed much higher costs than the Tennessee study. In 1992, Rose Dunn published a report based on her experience as a manager of medical records. She estimated a 10-page request would cost $5.32 in labor costs only, equaling labor cost per page of $0.53. However, this estimate appears to reflect costs before computerization. The expected time spent per search was 30.6 minutes; 85 percent of this time could be significantly reduced with computerization (this includes time taken for file retrieval, photocopying, and re-filing; file retrieval is the only time cost that would remain under computerization).

In estimating the cost of copying records, the Department relied on the public comment from a medical records outsourcing industry representative, which submitted specific volume and cost data from a major firm that provides extensive medical record copying services. According to these data, 900 million pages of medical records are copied each year in the U.S., the average medical record is 31 pages, and copying costs are $0.50 per page. In addition, the commenter noted that only 10 percent of all requests are made directly from patients, and of those, the majority are for purposes of continuing care (transfer to another provider), not for purposes of individual inspection. The Department assumed that 25 percent of direct patient requests to copy medical records are for purposes of inspecting their accuracy (i.e., 2.5 percent of all copy requests) or 850,000 in 2003 if the current practice remained unchanged.

To estimate the marginal increase in copying that might result from the regulation, the Department assumed that as patients gained more awareness of their right to inspect and copy their records, more requests will occur. As a result, the Department assumed a ten percent increase in the number of requests to inspect and copy medical records over the current baseline, which would amount to a little over 85,000 additional requests in 2003 at a cost of $1.3 million. Allowing for a 5.3 percent increase in records based on the increase in ambulatory care visits, the highest growth rate among health service sectors (the National Ambulatory Medical Care Survey, 1998), the total cost for the ten-year period would be $16.8 million.

The final rule allows a provider to deny an individual the right to inspect or obtain a copy of protected health information in a designated record set under certain circumstances, and it provides, in certain circumstances, that the patient can request the denial to be reviewed by another licensed health care professional. The initial provider can choose a licensed health care professional to render the second review.

The Department assumes denials and subsequent requests for reviews will be extremely rare. The Department estimates there are about 932,000 annual requests for inspections (*i.e.,* base plus new requests resulting from the regulation), or approximately 11 million over the ten-year period. If one-

tenth of one percent of these requests were to result in a denial in accordance with the rule, the result would be 11,890 cases. Not all these cases would be appealed. If 25 percent were appealed, the result would be 2,972 cases. If a second provider were to spend 15 minutes reviewing the case, the cost would be $6,000 in the first year and $86,360 over ten years.

Amendments to Protected Health Information

Many providers and health plans currently allow patients to amend the information in their medical record, where appropriate. If an error exists, both the patient and the provider or health plan benefit from the correction. However, as with inspection and copying, many states do not provide individuals with the right to request amendment to protected health information about themselves. Based on these assumptions, the Department concludes that the principal economic effect of the final rule would be to expand the right to request amendments to protected health information held by a health plan or provider to those who are not currently covered by amendment requirements under state laws or codes of conduct. In addition, the rule may draw additional attention to the issue of inaccuracies in information and may stimulate patient demand for amendment of medical records, including in those states that currently provide a right to amend medical records.

Under the final regulation, if a patient requests an amendment to his or her medical record, the provider must either accept the amendment or provide the individual with the opportunity to submit a statement disagreeing with the denial. The provider must acknowledge the request and inform the patient of his action.

The cost calculations assume that individuals who request an opportunity to amend their medical record have already obtained a copy of it. Therefore, the administrative cost of amending the patient's record is completely separate from inspection and copying costs.

Based on fact-finding discussions with a variety of providers, the Department assumes that 25 percent of the projected 850,000 people who request to inspect their records will seek to amend them. This number is the existing demand plus the additional requests resulting from the rule. Over ten years, the number of expected amendment requests will be 2.7 million. Unlike inspections, which currently occur in a small percentage of cases, our fact-finding suggests that patients very rarely seek to amend their records, but that the establishment of this right in the rule will spur more requests. The 25 percent appears to be high based on our discussions with providers but it is being used to avoid an underestimation of the cost.

As noted, the provider or health plan is not required to evaluate any amendment requests, only to append or otherwise link to the request in the record. We expect the responses will vary: sometimes an assistant will only make the appropriate notation in the record, requiring only a few minutes; other times a provider or manager will review the request and make changes if appropriate, which may require as much as an hour. To be conservative in its estimate, the Department has assumed, on average, 30 minutes for each amendment request at a cost of $47.28 per hour (2000 CPS).

The first-year cost for the amendment policy is estimated to be $5 million. The ten-year cost of this provision is $78.8 million.

Law Enforcement and Judicial and Administrative Proceedings

The law enforcement provisions of the final rule allow disclosure of protected health information without patient authorization under four circumstances: (1) Pursuant to legal process or as otherwise required by law; (2) to locate or identify a suspect, fugitive, material witness, or missing person; (3) under specified conditions regarding a victim of crime; and (4) and when a covered entity believes the protected health information constitutes evidence of a crime committed on its premises. As under current law and practice, a covered entity may disclose protected health information to a law enforcement official if such official.

Based on our fact finding, we are not able to estimate any additional costs from the final rule regarding disclosures to law enforcement officials. The final rule makes clear that current court orders and grand jury subpoenas will continue to provide a basis for covered entities to disclose protected health information to law enforcement officials. The three-part test, which covered entities must use to decide whether to disclose information in response to an administrative request such as an administrative subpoena, represents a change from current practice. There will be only minimal costs to draft the standard language for such subpoenas. We are unable to estimate other costs attributable to the use of administrative subpoenas. We have not been able to discover any specific information about the costs to law enforcement of establishing the predicates for issuing the administrative subpoena, nor have we been able to estimate the number of such subpoenas that will likely be issued once the final rule is implemented.

A covered entity may disclose protected health information in response to an order in the course of a judicial or administrative proceeding if reasonable efforts have been made to give the individual, who is the subject of the protected health information, notice of and an opportunity to object to the disclosure or to secure a qualified protective order.

The Department was unable to estimate any additional costs due to compliance with the final rule's provisions regarding judicial and administrative proceedings. The provision requiring a covered entity to make efforts to notify an individual that his or her records will be used in proceedings is similar to current practice; attorneys for plaintiffs and defendants agreed that medical records are ordinarily produced after the relevant party has been notified. With regard to protective orders, we believe that standard language for such orders can be created at minimal cost. The cost of complying with such protective orders will also likely be minimal, because attorney's client files are ordinarily already treated under safeguards comparable to those contemplated under the qualified protective orders. The Department was unable to make an estimate of how many such protective orders might be created annually.

We thus do not make any estimate of the initial or ongoing costs for judicial, administrative, or law enforcement proceedings.

Costs to the Federal Government

The rule will have a cost impact on various federal agencies that administer programs that require the use of individual health information. The federal costs of complying with the regulation and the costs when federal government entities are serving as providers are included in the regulation's total cost estimate outlined in the impact analysis. Federal agencies or programs clearly affected by the rule are those that meet the definition of a covered entity. However, non-covered agencies or programs that handle medical information, either under permissible exceptions to the disclosure rules or through an individual's expressed authorization, will likely incur some costs complying with provisions of this rule. A sample of federal agencies encompassed by the

broad scope of this rule include the: Department of Health and Human Services, Department of Defense, Department of Veterans Affairs, Department of State, and the Social Security Administration.

The greatest cost and administrative burden on the federal government will fall to agencies and programs that act as covered entities, by virtue of being either a health plan or provider. Examples include the Medicare, Medicaid, Children's Health Insurance and Indian Health Service programs at the Department of Health and Human Services; the CHAMPVA health program at the Department of Veterans Affairs; and the TRICARE health program at the Department of Defense. These and other health insurance or provider programs operated by the federal government are subject to requirements placed on covered entities under this rule, including, but not limited to, those outlined in Section D of the impact analysis. While many of these federal programs already afford privacy protections for individual health information through the Privacy Act and standards set by the Departments and implemented through their contracts with providers, this rule is nonetheless expected to create additional requirements. Further, we anticipate that most federal health programs will, to some extent, need to modify their existing practices to comply fully with this rule. The cost to federal programs that function as health plans will be generally the same as those for the private sector.

A unique cost to the federal government will be in the area of enforcement. The Office for Civil Rights (OCR), located at the Department of Health and Human Services, has the primary responsibility to monitor and audit covered entities. OCR will monitor and audit covered entities in both the private and government sectors, will ensure compliance with requirements of this rule, and will investigate complaints from individuals alleging violations of their privacy rights. In addition, OCR will be required to recommend penalties and other remedies as part of their enforcement activities. These responsibilities represent an expanded role for OCR. Beyond OCR, the enforcement provisions of this rule may have additional costs to the federal government through increased litigation, appeals, and inspector general oversight.

Examples of other unique costs to the federal government may include such activities as public health surveillance at the Centers for Disease Control and Prevention, health research projects at the Agency for Healthcare Research and Quality, clinical trials at the National Institutes of Health, and law enforcement investigations and prosecutions by the Federal Bureau of Investigations. For these and other activities, federal agencies will incur some costs to ensure that protected health information is handled and tracked in ways that comply with the requirements of this title.

We estimate that federal costs under this rule will be approximately $196 million in 2003 and $1.8 billion over ten years. The ten-year federal cost estimate represents about 10.2 percent of the privacy regulation's total cost. This estimate was derived in two steps.

First, we assumed that the proportion of the privacy regulation's total cost accruing to the federal government in a given year will be equivalent to the proportion of projected federal costs as a percentage of national health expenditures for that year. To estimate these proportions, we used the Health Care Financing Administration's November 1998 National Health Expenditure projections (the most recent data available) of federal health expenditures as a percent of national health expenditures from 2003 through 2008, trended forward to 2012. We then adjusted these proportions to exclude Medicare and Medicaid spending, reflecting the fact that the vast majority of participating Medicare and Medicaid providers will not be able to pass through the costs of complying with this rule to the federal government because they are not reimbursed under cost-based payment systems. This calculation yields a partial federal cost of $166 million in 2003 and $770 million over ten years.

Second, we add the Medicare and federal Medicaid costs resulting from the privacy regulation that HCFA's Office of the Actuary project can be passed through to the federal government. These costs reflect the actuaries' assumption regarding how much of the total privacy regulation cost burden will fall on participating Medicare and Medicaid providers, based on the November 1998 National Health Expenditure data. Then the actuaries estimate what percentage of the total Medicare and federal Medicaid burden could be billed to the programs, assuming that (1) only 3 percent of Medicare providers and 5 percent of Medicaid providers are still reimbursed under cost-based payment systems, and (2) over time, some Medicaid costs will be incorporated into the state's Medicaid expenditure projections that are used to develop the federal cost share of Medicaid spending. The results of this actuarial analysis add another $30 million in 2003 and $1.0 billion over ten years to the federal cost estimate. Together, these three steps constitute the total federal cost estimate of $236 million in 2003 and $2.2 billion over ten years.

Costs to State and Local Governments

The rule will also have a cost effect on various state and local agencies that administer programs requiring the use of individually identifiable health information. State and local agencies or programs clearly affected by the rule are those that meet the definition of a covered entity. The costs when government entities are serving as providers are included in the total cost estimates. However, non-covered agencies or programs that handle individually identifiable health information, either under permissible exceptions to the disclosure rules or through an individual's expressed authorization, will likely incur some costs complying with provisions of this rule. Samples of state and local agencies or programs encompassed by the broad scope of this rule include: Medicaid, State Children's Health Insurance Programs, county hospitals, state mental health facilities, state or local nursing facilities, local health clinics, and public health surveillance activities, among others. We have included state and local costs in the estimation of total costs in this section.

The greatest cost and administrative burden on the state and local government will fall to agencies and programs that act as covered entities, by virtue of being either a health plan or provider, such as Medicaid, State Children's Health Insurance Programs, and county hospitals. These and other health insurance or provider programs operated by state and local government are subject to requirements placed on covered entities under this rule, including, but not limited to, those outlined in this section (Section E) of the impact analysis. Many of these state and local programs already afford privacy protections for individually identifiable health information through the Privacy Act. For example, state governments often become subject to Privacy Act requirements when they contract with the federal government. This rule is expected to create additional requirements beyond those covered by the Privacy Act. Furthermore, we anticipate that most state and local health programs will, to some extent, need to modify their existing Privacy Act practices to fully comply with this rule. The cost to state

and local programs that function as health plans will be different than the private sector, much as the federal costs vary from private health plans.

A preliminary analysis suggests that state and local government costs will be on the order of $460 million in 2003 and $2.4 billion over ten years. We assume that the proportion of the privacy regulation's total cost accruing to state and local governments in a given year will be equivalent to the proportion of projected state and local costs as a percentage of national health expenditures for that year. To estimate these proportions, we used the Health Care Financing Administration's November 1998 National Health Expenditure projections of state and local health expenditures as a percent of national health expenditures from 2003 through 2008, trended forward to 2012. Based on this approach, we assume that over the entire 2003 to 2012 period, 13.6 percent, or $2.4 billion, of the privacy regulation's total cost will accrue to state and local governments. Of the $2.4 billion state and local government cost, 19 percent will be incurred in the regulation's first year (2003). In each of the out-years (2004–2012), the average percent of the total cost incurred will be about nine percent per year. These state and local government costs are included in the total cost estimates discussed in the regulatory impact analysis.

F. Benefits

There are important societal benefits associated with improving health information privacy. Confidentiality is a key component of trust between patients and providers, and some studies indicate that a lack of privacy may deter patients from obtaining preventive care and treatment.[52] For these reasons, traditional approaches to estimating the value of a commodity cannot fully capture the value of personal privacy. It may be difficult for individuals to assign value to privacy protection because most individuals view personal privacy as a right. Therefore, the benefits of the proposed regulation are impossible to estimate based on the market value of health information alone. However, it is possible to evaluate some of the benefits that may accrue to individuals as a result of proposed regulation, and these benefits, alone, suggest that the regulation is warranted. Added to these benefits is the intangible value of privacy, the security that individuals feel when personal information is kept confidential. This benefit is very real and very significant but there are no reliable means of measuring dollar value of such benefit.

As noted in the comment and response section, a number of commenters raised legitimate criticisms of the Department's approach to estimating benefits. The Department considered other approaches, including attempts to measure benefits in the aggregate rather than the specific examples set forth in the NPRM. However, we were unable to identify data or models that would provide credible measures. Privacy has not been studied empirically from an economic perspective, and therefore, we concluded that the approach taken in the NPRM is still the most useful means of illustrating that the benefits of the regulation are significant in relation to the economic costs.

Before beginning the discussion of the benefits, it is important to create a framework for how the costs and benefits may be viewed in terms of individuals rather than societal aggregates. We have estimated the value an insured individual would need to place on increased privacy to make the privacy regulation a net benefit to those who receive health insurance. Our estimates are derived from data produced by the 1998 Current Population Survey from the Census Bureau (the most recent available at the time of the analysis), which show that 220 million persons are covered by either private or public health insurance. Joining the Census Bureau data with the costs calculated in Section E, we have estimated the cost of the regulation to be approximately $6.25 per year (or approximately $0.52 per month) for each insured individual (including people in government programs). If we assume that individuals who use the health care system will be willing to pay more than this per year to improve health information privacy, the benefits of the proposed regulation will outweigh the cost.

This is a conservative estimate of the number of people who will benefit from the regulation because it assumes that only those individuals who have health insurance or are in government programs will use medical services or benefit from the provisions of the proposed regulation. Currently, there are 42 million Americans who do not have any form of health care coverage. The estimates do not include those who pay for medical care directly, without any insurance or government support. By lowering the number of users in the system, we have inflated our estimate of the per-person cost of the regulation; therefore, we assume that our estimate represents the highest possible cost for an individual.

An alternative approach to determining how people would have to value increased privacy for this regulation to be beneficial is to look at the costs divided by the number of encounters with health care professionals annually. Data from the Medical Expenditure Panel Survey (MEPS) produced by the Agency for Healthcare Policy Research (AHCPR) show approximately 776.3 million health care visits (*e.g.,* office visits, hospital and nursing home stays, etc.) in the first year (2003). As with the calculation of average annual cost per insured patient, we divided the total cost of complying with the regulation by the total annual number of health care visits. The cost of instituting requirements of the proposed regulation is $0.19 per health care visit. If we assume that individuals would be willing to pay more than $0.19 per health care visit to improve health information privacy, the benefits of the proposed regulation outweigh the cost.

Qualitative Discussion

A well designed privacy standard can be expected to build confidence among the public about the confidentiality of their medical records. The seriousness of public concerns about privacy in general are shown in the 1994 Equifax-Harris Consumer Privacy Survey, where ''84 percent of Americans are either very or somewhat concerned about threats to their personal privacy.'' [53] A 1999 report, ''Promoting Health and Protecting Privacy'' notes ''* * * many people fear their personal health information will be used against them: to deny insurance, employment, and housing, or to expose them to unwanted judgements and scrutiny.'' [54] These concerns would be partly allayed by the privacy standard.

Fear of disclosure of treatment is an impediment to health care for many Americans. In the 1993 Harris-Equifax Health Information Privacy Survey, seven percent of respondents said they or a member of their immediate family had chosen not to seek medical services due to fear of harm to job prospects or other life opportunities. About two percent reported having chosen not to file an insurance claim because of concerns of lack of privacy or confidentiality.[55] Increased confidence

[52] Equifax-Harris Consumer Privacy Survey, 1994.

[53] *Consumer Privacy Survey,* Harris-Equifax, 1994, p vi.

[54] *Promoting Health: Protecting Privacy,* California Health Care Foundation and Consumers Union, January 1999, p 12.

[55] *Health Information Survey,* Harris-Equifax, 1993, pp 49–50.

on the part of patients that their privacy would be protected would lead to increased treatment among people who delay or never begin care, as well as among people who receive treatment but pay directly (to the extent that the ability to use their insurance benefits will reduce cost barriers to more complete treatment). It will also change the dynamic of current payments. Insured patients currently paying out-of-pocket to protect confidentiality will be more likely to file with their insurer and to seek all necessary care. The increased utilization that would result from increased confidence in privacy could be beneficial under many circumstances. For many medical conditions, early and comprehensive treatment can lead to lower costs.

The following are four examples of areas where increased confidence in privacy would have significant benefits. They were chosen both because they are representative of widespread and serious health problems, and because they are areas where reliable and relatively complete data are available for this kind of analysis. The logic of the analysis, however, applies to any health condition, including relatively minor conditions. We expect that some individuals might be concerned with maintaining privacy even if they have no significant health problems because it is likely that they will develop a medical condition in the future that they will want to keep private.

Cancer

The societal burden of disease imposed by cancer is indisputable. Cancer is the second leading cause of death in the US,[56] exceeded only by heart disease. In 2000, it is estimated that 1.22 million new cancer cases will be diagnosed.[57] The estimated prevalence of cancer cases (both new and existing cases) in 1999 was 8.37 million.[58] In addition to mortality, incidence, and prevalence rates, the other primary methods of assessing the burden of disease are cost-of-illness and quality of life measures.[59] Cost of illness measures the economic costs associated with treating the disease (direct costs) and lost income associated with morbidity and mortality (indirect costs). The National Institutes of Health estimates that the overall annual cost of cancer in 1990 was $96.1 billion; $27.5 billion in direct medical costs and $68.7 billion for lost income due to morbidity and mortality.[60] Health-related quality of life measures integrate the mortality and morbidity effects of disease to produce health status scores for an individual or population. For example, the Quality Adjusted Life Year (QALY) combines the pain, suffering, and productivity loss caused by illness into a single measure. The Disability Adjusted Life Year (DALY) is based on the sum of life years lost to premature mortality and years that are lived, adjusted for disability.[61] The analysis below is based on the cost-of-illness measure for cancer, which is more developed than the quality of life measure.

Among the most important elements in the fight against cancer are screening, early detection and treatment of the disease. However, many patients are concerned that cancer detection and treatment will make them vulnerable to discrimination by insurers or employers. These privacy concerns have been cited as a reason patients do not seek early treatment for diseases such as cancer. As a result of forgoing early treatment, cancer patients may ultimately face a more severe illness and/or premature death.

Increasing people's confidence in the privacy of their medical information would encourage more people with cancer to seek cancer treatment earlier, which would increase cancer survival rates and thus reduce the lost wages associated with cancer. For example, only 24 percent of ovarian cancers are diagnosed in the early stages. Of these, approximately 90 percent of patients survive treatment. The survival rate of women who detect breast cancer early is similarly high; more than 90 percent of women who detect and treat breast cancer in its early stages will survive.[62]

We have attempted to estimate the annual savings in foregone wages that would result from earlier treatment due to enhanced protection of the privacy of medical records. We do not assume there would be increased medical costs from earlier treatment because the costs of earlier and longer cancer treatment are probably offset by the costs of treating late-stage cancer among people who would otherwise not be treated until their cases had progressed.

Although figures on the number of individuals who avoid cancer treatment due to privacy concerns do not exist, some indirect evidence is available. A 1993 Harris-Equifax Health Information Privacy Survey (noted earlier) found that seven percent of respondents reported that they or a member of their immediate family had chosen not to seek services for a physical or mental health condition due to fear of harm to job prospects or other life opportunities. It should be noted that this survey is somewhat dated and represents only one estimate. Moreover, given the wording of the question, there are other reasons aside from privacy concerns that led these individuals to respond affirmatively. However, for the purposes of this estimate, we assume that privacy concerns were responsible for the majority of positive responses.

Based on the Harris-Equifax survey estimate that seven percent of people did not seek services for physical or mental health conditions due to fears about job prospects or other opportunities, we assume that the proportion of people diagnosed with cancer who did not seek earlier treatment due to these fears is also seven percent. Applying this seven percent figure to the estimated number of total cancer cases (8.37 million) gives us an estimate of 586,000 people who did not seek earlier cancer treatment due to privacy concerns. We estimate annual lost wages due to cancer morbidity and mortality per cancer patient by dividing total lost wages ($68.7 billion) by the number of cancer patients (8.37 million), which rounds to $8,200. We then assume that cancer patients who seek earlier treatment would achieve a one-third reduction in cancer mortality and morbidity due to earlier treatment. The assumption of a one-third reduction in mortality and morbidity is derived from a study showing a one-third reduction in colorectal cancer mortality due to colorectal cancer screening.[63] We could have chosen a lower or higher treatment success rate. By multiplying 586,000 by $8,200 by one-third, we calculate that $1.6 billion in lost wages could be saved each year by encouraging more people to seek early cancer treatment through enhanced privacy protections. This estimate illustrates the potential savings

[56] American Cancer Society. http://4a2z.com/cgi/rfr.cgi?4CANCER–2-http://www.cancer.org/frames.html

[57] American Cancer Society. http://www3.cancer.org/cancerinfo/sitecenter.asp?ctid=8&scp= 0&scs= 0&scss= 0&scdoc = 40000.

[58] Polednak, AP. ''Estimating Prevalence of Cancer in the United States,'' Cancer 1997; 8–:136–41

[59] Martin Brown, ''The Burden of Illness of Cancer: Economic Cost and Quality of Life.'' Annual Review of Public Health, 2001:22:91–113.

[60] Disease-Specific Estimates of Direct and Indirect Costs of Illness and NIH Support: Fiscal Year 2000 Update. Department of Health and Human Services, Naitonal Institutes of Health, Office of the Director, February 2000.

[61] DALY scores for 10 cancer sites are presented in Brown, ''The Burden of Illness of Cancer: Economic Cost and Quality of Life,'' figure 1.

[62] Breast Cancer Information Service. http://trfn.clpgh.org/bcis/FAQ/facts2.html

[63] Jack S. Mandel, *et al.,* ''Reducing Mortality from Colorectal Cancer by Screening for Fecal Occult Blood,'' The New England Journal of Medicine, May 13, 1993, Vol, 328, No. 19.

in lost wages due to cancer that could be achieved with greater privacy protections.

HIV/AIDS

Early detection is essential for the survival of a person with HIV (Human Immunodeficiency Virus). Concerns about the confidentiality of HIV status would likely deter some people from getting tested. For this reason, each state has passed some sort of legislation regarding confidentiality of an individual's HIV status. However, HIV status can be revealed indirectly through disclosure of HAART (Highly Active Anti-Retroviral Therapy) or similar HIV treatment drug use. In addition, since HIV/AIDS (Acquired Immune Deficiency Syndrome) is often the only specially protected condition, ''blacked out'' information on medical charts could indicate HIV positive status.[64] Strengthening privacy protections beyond this disease could increase confidence in privacy regarding HIV as well. Drug therapy for HIV positive persons has proven to be a life-extending, cost-effective tool.[65] A 1998 study showed that beginning treatment with HAART in the early asymptomatic stage is more cost-effective than beginning it late. After five years, only 15 percent of patients with early treatment are estimated to develop an ADE (AIDS-defining event), whereas 29 percent would if treatment began later. Early treatment with HAART prolongs survival (adjusted for quality of life) by 6.2 percent. The overall cost of early HAART treatment is estimated at $23,700 per quality-adjusted year of life saved.[66]

Other Sexually Transmitted Diseases

It is difficult to know how many people are avoiding testing for STDs despite having a sexually transmitted disease. A 1998 study by the Kaiser Family Foundation found that the incidence of disease was 15.3 million in 1996, though there is great uncertainty due to under-reporting.[67] For a potentially embarrassing disease such as an STD, seeking treatment requires trust in both the provider and the health care system for confidentiality of such information. Greater trust should lead to more testing and greater levels of treatment. Earlier treatment for curable STDs can mean a decrease in morbidity and the costs associated with complications. These include expensive fertility problems, fetal blindness, ectopic pregnancies, and other reproductive complications.[68] In addition, there could be greater overall savings if earlier treatment translates into reduced spread of infections.

Mental Health Treatment

When individuals have a better understanding of the privacy practices that we are requiring in this proposed rule, some will be less reluctant to seek mental health treatment. One way that individuals will receive this information is through the notice requirement. Increased use of mental health and services would be expected to be beneficial to the persons receiving the care, to their families, and to society at large. The direct benefit to the individual from treatment would include improved quality of life, reduced disability associated with mental conditions, reduced mortality rate, and increased productivity associated with reduced disability and mortality. The benefit to families would include quality of life improvements and reduced medical costs for other family members associated with abusive behavior by the treated individual.

The potential economic benefits associated with improving privacy of individually identifiable health information and thus encouraging some portion of individuals to seek initial mental health treatment or increase service use are difficult to quantify well. Nevertheless, using a methodology similar to the one used above to estimate potential savings in cancer costs, one can lay out a range of possible benefit levels to illustrate the possibility of cost savings associated with an expansion of mental health and treatment to individuals who, due to protections offered by the privacy regulation, might seek treatment that they otherwise would not have. This can be illustrated by drawing upon existing data on the economic costs of mental illness and the treatment effectiveness of interventions.

The 1998 Substance Abuse and Mental Health Statistics Source Book from the Substance Abuse and Mental Health Services Administration (SAMHSA) estimates that the economic cost to society of mental illness in 1994 was about $204.4 billion. About $91.7 billion was due to the cost of treatment and medical care and $112.6 billion (1994 dollars) was due to loss of productivity associated with morbidity and mortality and other related costs, such as crime.[69] Evidence suggests that appropriate treatment of mental health disorders can result in 50–80 percent of individuals experiencing improvements in these types of conditions. Improvements in patient functioning and reduced hospital stays could result in hundreds of millions of dollars in cost savings annually.

Although figures on the number of individuals who avoid mental health treatment due to privacy concerns do not exist, some indirect evidence is available. As noted in the cancer discussion, the 1993 Harris-Equifax Health Information Privacy Survey found that 7 percent of respondents reported that they or a member of their immediate family had chosen not to seek services for a physical or mental health condition due to fear of harm to job prospects or other life opportunities. (See above for limitations to this data).

We assume that the proportion of people with a mental health disorder who did not seek treatment due to fears about job prospects or other opportunities is the same as the proportion in the Harris-Equifax survey sample who did not seek services for physical or mental health conditions due to the same fears (7 percent). The 1999 Surgeon General's Report on Mental Health estimates that 28 percent of the U.S. adult population has a diagnosable mental and/or substance abuse disorder and 20 percent of the population has a mental and/or substance abuse disorder for which they do not receive treatment.[70] Based on the Surgeon General's Report, we estimate that 15 percent of the adult population has a mental disorder for which they do not seek treatment.[71] Assuming that 7

[64] *Promoting Health: Protecting Privacy,* California Health Care Foundation and Consumers Union, January 1999, p 13

[65] For example, Roger Detels, M.D., *et al.,* in ''Effectiveness of Potent Anti-retroviral Therapy. * * *'' JAMA, 1998; 280:1497–1503 note the impact of therapy on HIV persons with respect to lengthening the time to development of AIDS, not just delaying death in persons who already have AIDS.

[66] John Hornberger *et al.,* ''Early treatment with highly active anti-retroviral therapy (HAART) is cost-effective compared to delayed treatment,'' 12th World AIDS conference, 1998.

[67] *Sexually Transmitted Diseases in America,* Kaiser Family Foundation, 1998, p. 12.

[68] Standard Medical information; see *http://www.mayohealth.org* for examples.

[69] Substance Abuse and Mental Health Services Administration. *http://www.samhsa.gov/oas/srcbk/costs-02htm.* Source of data: DP Rice, Costs of Mental Illness (unpublished data).

[70] Department of Health and Human Services, Mental Health: A Report of the Surgeon General. Rockville, MD: 1999, page 408.

[71] According to the Surgeon General's Report, 28 percent of the adult population have either a mental or addictive disorder, whether or not they receive services: 19 percent have a mental disorder alone, 6 percent have a substance abuse disorder alone, and 3 percent have both. Subtracting the 3 percent who have both, about three-quarters of the population with either a mental or addictive disorder have a mental disorder and one-quarter have a substance abuse disorder. We assume that this ratio (three-quarter to one-quarter) is the same for the adult population with either a mental or addictive disorder who do not receive services.

percent of those with mental disorders did not seek treatment due to privacy concerns, we estimate that 1.05 percent of the adult population [72] (15 percent multiplied by 7 percent), or 2.07 million people, did not seek treatment for mental illness due to privacy fears.

The indirect (non-treatment) economic cost of mental illness per person with mental illness is $2,590 ($112.6 billion divided by 43.4 million people with mental illness).[73] The treatment cost of mental illness per person with mental illness is $2,110 ($91.7 billion divided by 43.4 million individuals). If we assume that indirect economic costs saved by encouraging more individuals with mental illness to enter treatment are offset by the additional treatment costs, the net savings is about $480 per person.

As stated above, appropriate treatment of mental health disorders can result in 50-80 percent of individuals experiencing improvements in these types of conditions. Therefore, we multiply the number of individuals with mental disorders who would seek treatment with greater privacy protections (2.07 million) by the treatment effectiveness rate by the net savings per effective treatment ($480). Assuming a 50 percent success rate, this equation yields annual savings of $497 million. Assuming an 80 percent success rate, this yields annual savings of $795 million.

Given the existing data on the annual economic costs of mental illness and the rates of treatment effectiveness for these disorders, coupled with assumptions regarding the percentage of individuals who would seek mental health treatment with greater privacy protections, the potential net economic benefits could range from approximately $497 million to $795 million annually.

V. Final Regulatory Flexibility Analysis

A. Introduction

Pursuant to the Regulatory Flexibility Act 5 U.S.C. 601 *et seq.,* the Department must prepare a regulatory flexibility analysis if the Secretary certifies that a final rule would have a significant economic impact on a substantial number of small entities.[74]

This analysis addresses four issues: (1) The need for, and objective of, the rule; (2) a summary of the public comments to the NPRM and the Department's response; (3) a description and estimate of the number of small entities affected by the rule; and (4) a description of the steps the agency has taken to minimize the economic impact on small entities, consistent with the law and the intent of the rule. The following sections provide details on each of these issues. A description of the projected reporting and record keeping requirements of the rule are included in Section IX, below.

B. Reasons for Promulgating the Rule

This proposed rule is being promulgated in response to a statutory mandate to do so under section 264 of Public Law 104–191. Additional information on the reasons for promulgating the rule can be found in earlier preamble discussions (see Section I. B. above).

1. Objectives and Legal Basis

This information can be found in earlier preamble discussions (See I. C. and IV., above).

2. Relevant Federal Provisions

This information can be found in earlier preamble discussions (See I. C., above).

C. Summary of Public Comments

The Department received only a few comments regarding the Initial Regulatory Flexibility Analysis (IRFA) contained in the NPRM. A number of commenters argued that the estimates IRFA were too low or incomplete. The estimates were incomplete to the extent that a number of significant policy provisions in the proposal were not estimated because of too little information at the time. In the final IRFA we have estimates for these provisions. As for the estimates being too low, the Department has sought as much information as possible. The methodology employed for allocating costs to the small business sectors is explained in the following section.

Most of the other comments pertaining to the IRFA criticized specific estimates in the NPRM. Generally, the commenters argued that certain cost elements were not included in the cost estimates presented in the NPRM. The Department has expanded our description of our data and methodology in both the final RIA and this final RFA to try to clarify the data and assumptions made and the rationale for using them.

Finally, a number of commenters suggested that small entities be exempted from coverage from the final rule, or that they be given more time to comply. As the Department has explained in the Response to Comment section above, such changes were considered but rejected. Small entities constitute the vast majority of all entities that are covered; to exempt them would essentially nullify the purpose of the rule. Extensions were also considered but rejected. The rule does not take effect for two years, which is ample time for small entities to learn about the rule and make the necessary changes to come into compliance.

D. Economic Effects on Small Entities

1. Number and Types of Small Entities Affected

The Small Business Administration defines small businesses in the health care sector as those organizations with less than $5 million in annual revenues. Nonprofit organizations are also considered small entities;[75] however, individuals and states are not included in the definition of a small entity. Similarly, small government jurisdictions with a population of less than 50,000 are considered small entities.[76]

Small business in the health care sector affected by this rule may include such businesses as: Nonprofit health plans, hospitals, and skilled nursing facilities (SNFs); small businesses providing health coverage; small physician practices; pharmacies; laboratories; durable medical equipment (DME) suppliers; health care clearinghouses; billing companies; and vendors that supply software applications to health care entities.

The U.S. Small Business Administration reports that as of 1997, there were 562,916 small health care entities [77] classified within the SIC

Thus, we assume that 15 percent of the population have an untreated mental disorder (three-quarters of 20 percent) and 5 percent have an untreated addictive disorder (one-quarter of 20 percent).

[72] According to the Population Estimates Program, Population Division, U.S. Census Bureau, the U.S. population age 20 and older is 197.1 million on Sept. 1, 2000. This estimate of the adult population is used throughout this section.

[73] The number of adults with mental illness is calculated by multiplying the U.S. Census Bureau estimate of the U.S. adult population—197.1 million—by the percent of the adult population with mental illness—22 percent, according to the Surgeon General's Report on Mental Health, which says that 19 percent of the population have a mental disorder alone and three percent have a mental and substance abuse disorder.

[74] ''Entities'' and ''establishments'' are synonymous in this analysis.

[75] ''Entities'' and ''establishments'' are used synonymously in this RFA.

[76] ''Small governments'' were not included in this analysis directly; rather we have included the kinds of institutions within those governments that are likely to incur costs, such as government hospitals and clinics.

[77] Entities are the physical location where an enterprise conducts business. An enterprise may conduct business in more than one establishment.

codes we have identified as being covered establishments (Table A).

Table A.--Number of Health Care Establishments That Meet SBA Size Standards, 1997[1]

Standard Industrial Code (SIC)	Industry	Total Number of Health Care Establishments	Number of Establishments that Meet SBA Size Standards[2] or RFA non- profit standard	% of Establishments that Meet SBA Size Standards[2] or RFA non-profit standard
5910	Drug Stores & Proprietary Stores	48,147	23,923	49.7%
6320	Accident & Health Insurance & Medical Service Plans	8,083	665	8.2%
7352	Medical Equipment Rental and Leasing	3,346	1,836	54.9%
8010	Offices & Clinics Of Doctors Of Medicine	190,233	170,962	89.9%
8020	Offices & Clinics Of Dentists	115,020	113,864	99.0%
8030	Offices & Clinics Of Doctors Of Osteopathy	9,143	8,850	96.8%
8040	Offices & Clinics Of Other Health Practitioners	89,482	86,596	96.8%
8050	Nursing & Personal Care Facilities	33,178	17,727	53.4%
8060	Hospitals	6,991	3,485	49.8%
8070	Medical & Dental Laboratories	17,586	13,015	74.0%
8080	Home Health Care Services	19,562	12,841	65.6%
8090	Miscellaneous Health & Allied Services	22,145	11,219	50.7%
n/a	Fully Insured ERISA[2]	2,125,000	0	NA
n/a	Institutional Review Boards (IRB)[2]	450,000	0	NA
n/a	Total[2]	562,916	464,983	82.6%

1 Source: Office of Advocacy, U.S. Small Business Administration, from data provided by the Bureau of the Census, Statistics of U.S. Businesses, 1997. Establishments that have less than $5,000,000 in annual revenue are considered small businesses here, as are non-profit establishments (regardless of revenue). We have non-profit data for the following SICs: 8050, 8060, and 8080 and have included the number of non-profits in each category into the table.

[2] We have not included the number of fully insured ERISA plans or institutional review boards (IRB) in the total number of health care establishments or the number of establishments that meet SBA standards for small entities, since these are not separate businesses with SIC codes and we do not have sufficient data to impute revenues to them.

[3] We have included self-insured, self-administered plans and third party administrators in the total number of health plans, even though neither has individual SIC codes because we have the ability to impute revenues to them. Therefore, the number of health plans in SIC 6320 is greater than the figure usually reported in the Statistics of U.S. Businesses.

These small businesses represent 82.6% of all health care establishments examined.[78] Small businesses represent a significant portion of the total number of health care establishments but a small portion of the revenue stream for all health care establishments. In 1997, the small health care businesses represented generated approximately $430 billion in annual receipts, or 30.2% of the total revenue generated by health care establishments (Table B).[79] The following sections provide estimates of the number of small health care establishments that will be required to comply with the rule. Note, however, that the SBA's published annual receipts of health care industries differ from the National Health Expenditure data that the Health Care Financing Administration (HCFA) maintains.

[78] Office of Advocacy, U.S. Small Business Administration, from data provided by the Bureau of the Census, Statistics of U.S. Businesses, 1997.

[79] Op.cit, 1997.

These data do not provide the specific revenue data required for a RFA; only the SBA data has the requisite establishment and revenue data for this analysis.

Table B.--Annual Receipts of Health Care Entities, 1997[1]

Standard Industrial Code (SIC)	Industry	Total Revenue	Revenue Generated by Small Entities	% of Total Revenue Generated by Small Entities
5910	Drug Stores & Proprietary Stores	$100,302,441,000	$25,620,978,000	25.5%
6320	Accident & Health Insurance & Medical Service Plans (SIC 6320), Self-Insured/ Self Administered (no SIC), Third Party Administrators (no SIC)2	$512,111,493,027	$657,074,000	0.1%
7352	Medical Equipment Rental & Leasing	$4,040,646,000	$1,193,345,000	29.5%
8010	Offices & Clinics Of Doctors Of Medicine	$182,148,148,000	$105,334,031,000	57.8%
8020	Offices & Clinics Of Dentists	$48,766,434,000	$47,218,844,000	96.8%
8030	Offices & Clinics Of Doctors Of Osteopathy	$4,613,192,000	$4,039,868,000	87.6%
8040	Offices & Clinics Of Other Health Practitioners	$28,110,189,000	$23,170,899,000	82.4%
8050	Nursing & Personal Care Facilities	$77,166,537,000	$24,484,098,431	31.7%
8060	Hospitals	$382,540,791,000	$172,552,388,454	45.1%
8070	Medical & Dental Laboratories	$19,872,150,000	$6,862,628,000	34.5%
8080	Home Health Care Services	$31,061,036,000	$12,085,755,906	38.9%
8090	Miscellaneous Health & Allied Services	$35,034,774,000	$6,812,006,000	19.4%
N/A	Total Receipts	$1,425,767,831,027	$430,031,915,791	30.2%

1 Source: Office of Advocacy, U.S. Small Business Administration, from data provided by the Bureau of the Census, Statistics of U.S. Businesses, 1997. Entities that have less than $5,000,000 in annual revenue are considered small businesses here, as are non-profit entities (regardless of revenue). We have non-profit data for the following SICs: 8050, 8080, and 8060 and have included the number of non-profits in each category into the table.

2 We have included self-insured/self-administered plans and third party administrators in the total number of health plans, even though neither has individual SIC codes because we have the ability to impute revenues to them.

The Small Business Administration reports that approximately 74 percent of the 18,000 medical laboratories and dental laboratories in the U.S. are small entities.[80] Furthermore, based on SBA data, 55 percent of the 3,300 durable medical equipment suppliers that are not part of drug and proprietary stores in the U.S. are small entities. Over 90 percent of health practitioner offices are small businesses.[81] Doctor offices (90%), dentist offices (99%), osteopathy (97%) and other health practitioner offices (97%) are primarily considered small businesses.

There are also a number of hospitals, home health agencies, non-profit nursing facilities, and skilled nursing facilities that will be affected by the proposed rule. According to the American Hospital Association, there are approximately 3,131 nonprofit hospitals nationwide. Additionally, there are 2,788 nonprofit home health agencies in the U.S. and the Health Care Financing Administration reports that there are 591 nonprofit nursing facilities and 4,280 nonprofit skilled nursing facilities.[82]

Some contractors that are not covered entities but that work with covered health care entities will be required to adopt policies and procedures to protect information. We do not expect that the additional burden placed on contractors will be significant. We have not estimated the effect of the proposed rule on these entities because we cannot reasonably anticipate the number or type of contracts affected by the proposed rule. We also do not know the extent to which contractors would be required to modify their policy practices as a result of the rule.

2. Activities and Costs Associated With Compliance

This section summarizes specific activities that covered entities must undertake to comply with the rule's provisions and options considered by the Department that would reduce the burden to small entities. In developing this rule, the Department considered a variety of alternatives for minimizing the economic burden that it will create for small entities. We did not exempt small businesses from the rule because they represent such a large and critical proportion of the health care industry (82.6 percent); a significant portion of individually identifiable health information is generated or held by these small businesses.

The guiding principle in our considerations of how to address the burden on small entities has been to make provisions performance rather than specification oriented—that is, the rule states the standard to be achieved but allows institutions flexibility to determine how to achieve the standard within certain parameters. Moreover, to the extent possible, we have allowed entities to determine the extent to which they will address certain issues. This ability to adapt provisions to minimize burden has been addressed in the regulatory impact analysis above, but it will be briefly discussed again in the following section.

Before discussing specific provisions, it is important to note some of the broader questions that were addressed in formulating this rule. The Department considered extending the compliance period for small entities but concluded that it did not have the legal authority to do so (see discussion above). The rule, pursuant to HIPAA, creates an extended compliance time of 36 months (rather than 24 months) only for small health plans and not for other small entities. The Department also considered giving small entities longer response times for time limits set forth in the rule, but decided to establish standard time limits that we believe are reasonable for covered entities of all sizes, with the understanding that larger entities may not need as much time as they have been allocated in certain situations. This permits each covered entity the flexibility to establish policies regarding time limits that are consistent with the entity's current practices.

Although we considered the needs of small entities during our discussions of all provisions for this final rule, we are highlighting the most significant discussions in the following sections:

Scalability

Wherever possible, the final rule provides a covered entity with flexibility to create policies and procedures that are best suited to the entity's current practices in order to comply with the standards, implementation specifications, and requirements of the rule. This allows the covered entity to assess its own needs in devising, implementing, and maintaining appropriate privacy policies, procedures, and documentation to address these regulatory requirements. It also will allow a covered entity to take advantage of developments and methods for protecting privacy that will evolve over time in a manner that is best suited to that institution. This approach allows covered entities to strike a balance between protecting privacy of individually identifiable health information and the economic cost of doing so within prescribed boundaries set forth in the rule. Health care entities must consider both factors when devising their privacy solutions. The Department assumes that professional and trade associations will provide guidance to their members in understanding the rule and providing guidance on how they can best achieve compliance. This philosophy is similar to the approach in the Transactions Rule.

The privacy standard must be implemented by all covered entities, regardless of size. However, we believe that the flexible approach under this rule is more efficient and appropriate then a single approach to safeguarding health information privacy. For example, in a small physician practice, the office manager might be designated to serve as the privacy official as one of many of her duties. In a large health plan, the privacy official position may require more time and greater privacy experience, or the privacy official may have the regular support and advice of a privacy staff or board. The entity can decide how to implement this privacy official requirement based on the entity's structure and needs.

The Department decided to use this scaled approach to minimize the burden on all entities, with an emphasis on small entities. The varying needs and capacities of entities should be reflected in the policies and procedures adopted by the organization and the overall approach it takes to achieve compliance.

Minimum Necessary

The ''minimum necessary'' policy in the final rule has essentially three components: first, it does not pertain to certain uses and disclosures including treatment-related exchange of information among health care providers; second, for disclosures that are made on a routine basis, such as insurance claims, a covered entity is required to have policies and procedures governing such exchanges (but the rule does not require a case-by-case determination in such cases); and third, providers must have a process for reviewing non-routine requests on a case-by-case basis to assure that only the minimum necessary information is disclosed. The final rule makes changes to the NPRM that reduce the burden of compliance on small businesses.

Based on public comments and subsequent fact-finding, the Department sought to lessen the burden of this

[80] Office of Advocacy, U.S. Small Business Administration, from data provided by the Bureau of the Census, Statistics of U.S. Businesses, 1997.

[81] Op.cit., 1997.

[82] Health Care Financing Administration, OSCAR.

provision. The NPRM proposed applying the minimum necessary standard to disclosures to providers for treatment purposes and would have required individual review of all uses of protected health information. The final rule exempts disclosures of protected health information from a covered entity to a health care provider for treatment from the minimum necessary provision and eliminates the case-by-case determinations that would have been necessary under the NPRM. The Department has concluded that the requirements of the final rule are similar to the current practice of most health care providers. For standard disclosure requests, for example, providers generally have established procedures. Under the final rule providers will have to have policies and procedures to determine the minimum amount of protected health information to disclose for standard disclosure requests as well, but may need to review and revise existing procedures to make sure they are consistent with the final rule. For non-routine disclosures, providers have indicated that they currently ask questions to discern how much information should be disclosed. In short, the minimum necessary requirements of this rule are similar to current practice, particularly among small providers.

Policy and Procedures

The rule requires that covered entities develop and document policies and procedures with respect to protected health information to establish and maintain compliance with the regulation. Through the standards, requirements, and implementation specifications, we are proposing a framework for developing and documenting privacy policies and procedures rather than adopting a rigid, prescriptive approach to accommodate entities of different sizes, type of activities, and business practices. Small providers will be able to develop more limited policies and procedures under the rule, than will large providers and health plans, based on the volume of protected health information. We also expect that provider and health plan associations will develop model policies and procedures for their members, which will reduce the burden on small businesses.

Privacy Official

The rule requires covered entities to designate a privacy official who will be responsible for the development and implementation of privacy policies and procedures. The implementation of this requirement may vary based on the size of the entity. For example, a small physician's practice might designate the office manager as the privacy official in addition to her broader administrative responsibilities. Once the privacy official has been trained, the time required to accomplish the duties imposed on such person is not likely to be much more than under current practice. Therefore, the requirement imposes a minimal burden on small businesses.

Internal Complaints

The final rule requires covered entities to have an internal process for individuals to make complaints regarding the covered entities' privacy policies and procedures required by the rule and its compliance with such policies. The requirement includes identifying a contact person or office responsible for receiving complaints and documenting all complaints received and the disposition of such complaints, if any. The covered entity only is required to receive and document a complaint (the complaint can be oral or in writing), which should take a short amount of time. The Department believes that complaints about a covered entity's privacy policies and procedures will be uncommon. Thus, the burden on small businesses should be minimal.

Training

In developing the NPRM, the Department considered a number of alternatives for training, including requiring specific training materials, training certification, and periodic retraining. In the NPRM, the Department recommended flexibility in the materials and training method used, but proposed recertification every three years and retraining in the event of material changes in policy.

Based on public comment, particularly from small businesses, the Department has lessened the burden in the final rule. As in the proposal, the final rule requires all employees who are likely to have contact with protected health information to be trained. Covered entities will have to train employees by the compliance date specific to the type of covered entity and train new employees within a reasonable time of initial employment. In addition, a covered entity will have to train each member of its workforce whose functions are affected by a material change in the policies or procedures of such entity. However, the final rule leaves to the employer the decisions regarding the nature and method of training to achieve this requirement. The Department expects a wide variety of options to be made available by associations, professional groups, and vendors. Methods might include classroom instruction, videos, booklets, or brochures tailored to particular levels of need of workers and employers. Moreover, the recertification requirement of the NPRM has been dropped to ease the burden on small entities.

Consent

The NPRM proposed prohibiting covered entities from requiring individuals to provide written consent for the use and disclosure of protected health information for treatment, payment, and health care operations purposes. The final rule requires certain health care providers to obtain written consent before using or disclosing protected health information for treatment, payment, and health care operations, with a few exceptions. This requirement was included in the final rule in response to comments that this reflects current practice of health care providers health care providers with direct treatment relationships. Because providers are already obtaining such consent, this requirement represents a minimal burden.

Notice of Privacy Rights

The rule requires covered entities to prepare and make available a notice that informs individuals about uses and disclosures of protected health information that may be made by the covered entity and that informs of the individual's rights and covered entity's legal duties with respect to protected health information. The final rule makes changes to the NPRM that reduce the burden of this provision on covered entities and allows flexibility. The NPRM proposed that the notice describe the uses and disclosures of information that the entity *expected to make* without individual authorization. The final rule only requires that the notice describe uses and disclosures that the entity is permitted or required to make under the rule without an individual's written consent or authorization. This change will allow entities to use standardized notice language within a given state, which will minimize the burden of each covered entity preparing a notice. Professional associations may develop model language to assist entities in developing notices required by the rule. While the final rule specifies minimum notice requirements, it allows entities flexibility to add more detail about a covered entity's privacy policies.

The NPRM also proposed that health plans distribute the notice every three years. The final rule reduced this

burden by requiring health plans (in addition to providing notice to individuals at enrollment and prior to the compliance date of this rule) to inform individuals at least once every three years about the availability of the notice and how to obtain a copy rather than to distribute a copy of the notice.

In discussing the requirement for covered entities to prepare and make available a notice, we considered exempting small businesses (83 percent of entities) or extremely small entities (fewer than 10 employees). The Department decided that informing consumers of their privacy rights and of the activities of covered entities with which they conduct business was too important a goal of this rule to exempt any entities.

In addition to requiring a basic notice, we considered requiring a longer more detailed notice that would be available to individuals on request. However, we decided that it would be overly burdensome to all entities, especially small entities, to require two notice.

We believe that the proposed rule appropriately balances the benefits of providing individuals with information about uses and disclosures of protected health information with covered entities' need for flexibility in describing such information.

Access to Protected Health Information

The public comments demonstrate that inspection and copying of individually identifiable health information is wide-spread today. Individuals routinely request copies of such information, in whole or in part, for purposes that include providing health information to another health care provider or as part of legal proceedings. The amount of inspection and copying of individually identifiable health information that occurs for these purposes is not expected to change as a result of the final regulation.

The final regulation establishes the right of individuals to inspect and copy protected health information about them. Although this is an important right, the Department does not expect it to result in dramatic increases in requests from individuals. We assume that most health care providers currently have procedures for allowing patients to inspect and copy this information. The economic impact on small businesses of requiring covered entities to provide individuals with access to protected health information should be relatively small. Moreover, entities can recoup the costs of copying such information by charging reasonable cost-based fees.

Amendments to Protected Health Information

Many health care providers and health plans currently make provisions to help patients expedite amendments and corrections of their medical record where appropriate. If an error exists, both the patient and the health care provider on health plan benefit from the correction. However, as with inspection and copying, a person's right to request amendment and correction of individually identifiable health information about them is not guaranteed by all states. Based on these assumptions, the Department concludes that the principal economic effect of the final rule will be to expand the right to request amendments to protected health information held by health plans and covered health care providers to those who are currently granted such right by state law. In addition, the rule may draw additional attention to the issue of record inaccuracies and stimulate patient demand for amendment of medical records.

Under the final regulation, if an individual requests an amendment to protected health information about him or her, the health care provider must either accept the amendment or provide the individual with the opportunity to submit a statement disagreeing with the denial. We expect the responses to requests will vary; sometimes an assistant will only make the appropriate notation in the record, requiring only a few minutes; other times a health care provider or manager will review the request and make changes if appropriate, which may require as much as an hour.

Unlike inspections, which currently occur in a small percentage of cases, fact-finding suggests that individuals rarely seek to amend their records today, but the establishment of this right in the rule may spur more requests, including among those who in the past would have only sought to inspect their records. Nevertheless, we expect that the absolute number of additional amendment requests caused by the rule to be small (about 200,000 per per spread over more than 600,000 entities), which will impose only a minor burden on small businesses.

Accounting for Disclosures

The rule grants individuals the right to receive an accounting of disclosures made by a health care provider or plan for purposes other than treatment, payment, or health care operations, with certain exceptions such as disclosures to the individual. The individual may request an accounting of disclosures made up to six years prior to the request. In order to fulfill such requests, covered health care providers and health plans may track disclosures by making a notation in the individual's medical record regarding the (manual or electronic) when a disclosure is made. We have learned through fact-finding that some health care providers currently track various types of disclosures. Moreover, the Department does not expect many individuals will request an accounting of disclosures. Thus, this requirement will impose a minor burden on small businesses.

De-Identification of Information

In this rule, the Department allows covered entities to determine that health information is de-identified (*i.e.* that it is not individually identifiable health information), if certain conditions are met. Moreover, information that has been de-identified in accordance with the rule is not considered individually identifiable information and may be used or disclosed without regard to the requirements of the regulation. The covered entity may assign a code or other means of record identification to allow de-identified information to be re-identified if requirements regarding derivation and security are met.

As with other components of this rule, the approach used to remove identifiers from data can be scaled to the size of the entity. Individually identifiable health information can be de-identified in one of two ways; by either removing each of the identifiers listed in the rule or by engaging in a statistical and scientific analysis to determine that information is very unlikely to identify an individual. Small entities without the resources to conduct such an analysis can create de-identified information by removing the full list of possible identifiers set forth in this regulation. Unless the covered entity knows that the information could still identify an individual, the requirement of this rule would be fulfilled. However, larger, more sophisticated covered entities may close to determine independently what information needs to be removed based on sophisticated statistical and scientific analysis.

Efforts to remove identifiers from information are optional. If a covered entity can not use or disclose protected health information for a particular purpose but believes that removing identifiers is excessively burdensome, it can choose not to release the protected health information, or it can seek an authorization from individuals for the use or disclosure of protected health

information including some or all of the identifiers.

Finally, as discussed in the Regulatory Impact Analysis, the Department believes that very few small entities engage in de-identification currently. Fewer small entities are expected to engage in such activity in the future because the increasing trend toward computerization of large record sets will result in de-identification being performed by relatively few firms or associations over time. We expect that a small covered entity will find it more efficient to contract with specialists in large firms to de-identify protected health information. Larger entities are more likely to have both the electronic systems and the volume of records that will make them attractive for this business.

Monitoring Business Associates

The final rule requires a covered entity with a business associate to have a written contract or other arrangement that documents satisfactory assurance that the business associate will appropriately safeguard protected health information. The Department expects business associate contracts to be fairly standardized, except for language that will have to be tailored to the specific arrangement between the parties, such as the allowable uses and disclosures of information. The Department assumes the standard language initially will be developed by trade and professional associations for their members. Small health care providers are likely to simply adopt the language or make minor modifications. The regulation includes a requirement that the covered entity take steps to correct, and in some cases terminate, a contract, if necessary, if they know of violations by a business associate. This oversight requirement is consistent with standard oversight of a contract. The Department expects that most entities, particularly smaller ones, will utilize standard language that restricts uses and disclosures of individually identifiable health information their contracts with business associates. This will limit the burden on small businesses.

The NPRM proposed that covered entities be held accountable for the uses and disclosures of individually identifiable health information by their business associates. An entity would have been in violation of the rule if it knew of a breach in the contract by a business associate and failed to cure the breach or terminate the contract. The final rule reduces the extent to which an entity must monitor the actions of its business associates. The entity no longer has to ''ensure'' that each business associate complies with the rule's requirements. Entities will be required to cure a breach or terminate a contract for business associate actions only if they knew about a contract violation. The final rule is consistent with the oversight a business would provide for any contract, and therefore, the changes in the final rule will impose no new significant cost for small businesses in monitoring their business associates' behavior.

Employers With Insured Group Health Plans

Some group health plans will use or maintain individually identifiable health information, particularly group health plans that are self-insured. Also, some plan sponsors that perform administrative functions on behalf of their group health plans may need protected health information. The final rule permits a group health plan, or a health insurance issuer or HMO that provides benefits on behalf of the group health plan, to disclose protected health information to a plan sponsor who performs administrative functions on its behalf for certain purposes and if certain requirements are met. The plan documents must be amended to: describe the permitted uses and disclosures of protected health information by the plan sponsor; specify that disclosure is permitted only upon receipt of a certification by the plan sponsor that the plan documents have been amended and the plan sponsor agrees to certain restrictions on the use of protected health information; and provide for adequate firewalls to assure unauthorized personnel do not have access to individually identifiable health information.

Some plan sponsors may need information, not to administer the group health plan, but to amend, modify, or terminate the health plan. ERISA case law describes such activities as settlor functions. For example a plan sponsor may want to change its contract from a preferred provider organization to a health maintenance organization (HMO). In order to obtain premium information, the health plan sponsor may need to provide the HMO with aggregate claims information. Under the rule, the health plan sponsor can obtain summary information with certain identifiers removed, in order to provide it to the HMO and receive a premium rate.

The Department assumes that most health plan sponsors who are small employers (those with 50 or fewer employees) will elect not to receive individually identifiable health information because they will have little, if any, need for such data. Any needs that sponsors of small group health plans may have for information can be accomplished by receiving the information in summary form from their health insurance issuers.

3. The Burden on a Typical Small Business

The Department expects small entities to face a cost burden as a result of complying with the proposed regulation. We estimate that the burden of developing privacy policies and procedures is lower in dollar terms for small businesses than for large businesses, but we recognize that the cost of implementing privacy provisions could be a larger burden to small entities as a proportion of total revenue. Due to these concerns, we have relied on the principle of scalability throughout the rule, and have based our cost estimates on the expectation that small entities will develop less expensive and less complex privacy measures that comply with the rule than large entities.

In many cases, we have specifically considered the impact that rule may have on solo practitioners or rural health care providers. If a health care provider only maintains paper records and does not engage in any electronic transactions, the regulation would not apply to such provider. We assume that those providers will be small health care providers. For small health care providers that are covered health care providers, we expect that they will not be required to change their business practices dramatically, because we based many of the standards, implementation specifications, and requirements on current practice and we have taken a flexible approach to allow scalability based on a covered entity's activities and size. In developing policies and procedures to comply with the proposed regulation, scalability allows entities to consider their basic functions and the ways in which protected health information is used or disclosed. All covered entities must take appropriate steps to address privacy concerns, and in determining the scope and extent of their compliance activities, businesses should weigh the costs and benefits of alternative approaches and should scale their compliance activities to their structure, functions, and capabilities within the requirements of the rule.

Cost Assumptions

To determine the cost burden to small businesses of complying with the final rule, we used as a starting point the overall cost of the regulation determined

in the regulatory impact analysis (RIA). Then we adopted a methodology that apportions the costs found in the RIA to small business by using Census Bureau's Statistics of U.S. Businesses. This Census Bureau survey contains data on the number and proportion of establishments, by Standard Industrial Classification Code (SIC code), that have revenues of less than $5 million, which meets the Small Business Administration's definition of a small business in the health care sector. This data permitted us to calculate the proportion of the cost of each requirement in the rule that is attributable to small businesses. This methodology used for the regulatory flexibility analysis (RFA) section is therefore based on the methodology used in the (RIA), which was discussed earlier.

The businesses accounted for in the SIC codes contain three groups of covered entities: non-hospital health care providers, hospitals, and health plans. Non-hospital health care providers include: drug stores, offices and clinics of doctors, dentists, osteopaths, and other health practitioners, nursing and personal care facilities, medical and dental laboratories, home health care services, miscellaneous health and allied services, and medical equipment rental and leasing establishments. Health plans include accident and health insurance and medical service plans.

Data Adjustments

Several adjustments were made to the SIC code data to more accurately determine the cost to small and non-profit businesses. For health plans (SIC code 6320), we adjusted the SIC data to include self-insured, self-administered health plans because these health plans are not included in any SIC code, though they are covered entities under the rule. Similarly, we have added third-party administrators (TPAs) into this SIC. Although they are not covered entities, TPAs are likely to be business associates of covered entities. For purposes of the regulatory analyses, we have assumed that TPAs would bear many of the same costs of the health plans to assure compliance for the covered entity. To make this adjustment, we assumed the self-insured/self administered health plans and TPAs have the average revenue of the health plans contained in the SIC code, and then added those assumed revenues to the SIC code and to the total of all health care expenditures. Moreover, we needed to account for the cost to non-profit institutions that might receive more than $5 million in revenue, because all non-profit institutions are small businesses regardless of revenue. To make this adjustment for hospitals, nursing homes, and home health agencies, we used data on the number of non-profit institutions from industry sources and from data reported to HCFA. With this data, we assumed the current count of establishments in the SIC codes includes these non-profit entities and that non-profits have the same distribution of revenues as all establishments reported in the applicable SIC codes. The proportions discussed below, which determine the cost for small business, therefore include these non-profit establishments in SIC codes 8030, 8060, and 8080.

The SIC code tables provided in this RFA do not include several categories of businesses that are included in the total cost to small businesses. Claims clearinghouses are not included in the table because claims clearinghouses report their revenues under the SIC 7374 ''Computer Processing and Data Preparation,'' and the vast majority of businesses in this SIC code are involved in non-medical claims data processing. In addition, claims processing is often just one business-line of companies that may be involved in multiple forms of data processing, and therefore, even if the claims processing line of the business generates less than $5 million in revenue, the company in total may exceed the SBA definition for a small business (the total firm revenue, not each line of business, is the standard for inclusion). Similarly, fully-insured ERISA health plans sponsored by employers are not identified as a separate category in the SIC code tables because employers in virtually all SIC codes may sponsor fully-insured health plans. We have identified the cost for small fully-insured ERISA health plans by using the Department of Labor definition of a small ERISA plan, which is a plan with fewer than 100 insured participants. Using this definition, the initial cost for small fully-insured ERISA health plans is $7.1 million. Finally, Institutional Review Boards (IRBs) will not appear in a separate SIC code because IRBs are not ''businesses''; rather, they are committees of researchers who work for institutions where medical research is conducted, such as universities or teaching hospitals. IRB members usually serve as a professional courtesy or as part of their employment duties and are not paid separately for their IRB duties. Although IRBs are not ''businesses'' that generate revenues, we have treated them as small business for illustrative purposes in this RFA to demonstrate the additional opportunity costs that will be faced by those researchers who sit on IRBs. Therefore, assuming IRBs are small businesses, the initial costs are $.089 million and ongoing costs are approximately $84.2 million over 9 years.

The Cost Model Methodology

The RIA model employs two basic methodologies to determine the costs to small businesses that are covered entities. As stated above, the RFA determines the cost to small businesses by apportioning the total costs in the RIA using SIC code data. In places where the cost of a given provision of the final rule is a function of the number of covered entities, we determined the proportion of entities in each SIC code that have less than $5 million in revenues (see Table A). We then multiplied this proportion by the per-entity cost estimate of a given provision as determined in the RIA. For example, the cost of the privacy official provision is based on the fact that each covered entity will need to have a privacy official. Therefore, we multiplied the total cost of the privacy official, as determined in the RIA, by the proportion of small businesses in each SIC code to determine the small business cost. Using hospitals for illustrative purposes, because small and non-profit hospitals account for 50 percent of all hospitals, our methodology assigned 50 percent of the cost to small hospitals.

We used a second, though similar, method when the cost of a given provision in the RIA did not depend on the number of covered entities. For example, the requirement to provide notice of the privacy policy is a direct function of the number of patients in the health care system because the actual number of notices distributed depends on how many patients are seen. Therefore, for provisions like the notice requirement, we used SIC code revenue data in a two-step process. First, we apportioned the cost of each provision among sectors of the health care industry by SIC code. For example, because hospital revenue accounts for 27 percent of all health care revenue, we multiplied the total cost of each such provision by 27 percent to determine the cost for the hospital sector in total. Then to determine the cost for small hospitals specifically, we calculated the proportion by the overall cost. For example, 45.1 percent of all hospital revenue is generated by small hospital, therefore, the cost to small hospitals was assumed to account for 45.1 percent of all hospital costs. Estimates, by nature

are inexact. However, we feel this is a reasonable way to determine the small business costs attributable to this regulation given the limited data from which to work.

Total Costs and Costs Per Establishment for Small Business

Based on the methodology described above, the total cost of complying with the final rule in the initial year of 2003 is $1.9 billion. The ongoing costs to small business from 2004 to 2012 is $9.3 billion. Table C presents the initial and ongoing costs to small business by each SIC code. According to this table, small doctors offices, small dentists offices and small hospitals will face the highest cost of complying with the final rule. However, much of the reason for the higher costs faced by these three groups of small health care providers is explained by the fact that there are a significant number of health care providers in these categories.

BILLING CODE 4150–04–P

Table C.--Annual Cost to Small Business of Implementing Provisions of the Proposed Privacy Regulation[1]

SIC	Industry	Initial Cost (Year 1)[1]	Ongoing Cost (Year 2-10)	Total Costs
5910	Drug Stores & Proprietary Stores	$153,976,159	$780,573,862	$934,550,021
6320	Accident & Health Insurance & Medical Service Plans[2]	$41,348,527	$169,540,638	$210,889,164
7353	Medical Equipment Rental & Leasing	$7,171,728	$36,356,688	$43,528,416
8010	Offices & Clinics of Doctors of Medicine	$633,033,192	$3,209,127,747	$3,842,160,938
8120	Offices & Clinics of Dentists	$283,774,344	$1,438,578,786	$1,722,353,130
8030	Offices & Clinics of Doctors of Osteopathy	$24,278,673	$123,079,430	$147,358,103
8040	Offices & Clinics of Other Health Practitioners	$139,251,750	$705,929,263	$845,181,013
8050	Nursing & Personal Care Facilities	$147,143,775	$745,937,461	$893,081,236
8060	Hospitals	$355,459,094	$1,199,498,063	$1,554,957,157
8070	Medical & Dental Laboratories	$41,242,809	$209,078,203	$250,321,012
8080	Home Health Care Services	$72,632,601	$368,207,067	$440,839,668
8090	Misc Health & And Allied Services	$40,938,582	$207,535,943	$248,474,525
n/a	Fully Insured/ ERISA	$7,137,028	$0	$7,137,028
n/a	IRBs	$88,813	$84,162,446	$84,251,259
n/a	Total Cost For Small Business	$1,947,477,073	$9,277,605,598	$11,225,082,671

[1] Source: Office of Advocacy, U.S. Small Business Administration, from data provided by the Bureau of the Census, Statistics of U.S. Businesses, 1997. Entities that have less than $5,000,000 in annual revenue are considered small businesses here, as are non-profit entities (regardless of revenue). We have non-profit data for the following SICs: 8050, 8080, and 8060 and have included the number of non-profits in each category into the table.

[2] The initial costs include all costs in the first year, including costs that recur in subsequent years.

[3] We have included self-insured/self-administered health plans and third party administrators in the total number of health plans, even though neither has individual SIC codes because we have the ability to impute revenues to them.

On a per-establishment basis, Table D demonstrates that the average cost for small business of complying with the proposed rule in the first year is $4,188 per-establishment. The ongoing costs of privacy compliance are approximately $2,217 each year thereafter. We estimate that the average cost of compliance in the first year for each small non-hospital health care provider is approximately 0.6 percent of per-establishment revenues. In subsequent years, per-establishment costs about 0.3 percent of per-establishment revenues. For small hospitals and health plans, the per-establishment cost of compliance in the first year is 0.2 percent and 6.3 percent of per-establishment revenues respectively. For subsequent years, the cost is only 0.1 percent and 2.9 percent of pre-establishment revenues respectively. These costs may be offset in many firms by the savings realized through requirements of the Transactions Rule.

Table D.--Average Annual per Establishment Privacy Costs[1]

SIC	Industry	Year 1 Privacy Costs Per Establishment	Average Year 2-10 Privacy Costs per Establishment
5910	Drug Stores & Proprietary Stores	$6,436	$3,625
6320	Accident & Health Insurance & Medical Service Plans[2]	$62,162	$28,320
7353	Medical Equipment Rental & Leasing	$3,906	$2,200
8010	Offices & Clinics of Doctors of Medicine	$3,703	$2,086
8120	Offices & Clinics of Dentists	$2,492	$1,404
8030	Offices & Clinics of Doctors of Osteopathy	$2,743	$1,545
8040	Offices & Clinics of Other Health Practioners	$1,608	$906
8050	Nursing & Personal Care Facilities	$8,301	$4,676
8060	Hospitals	$101,999	$38,244
8070	Medical & Dental Laboratories	$3,169	$1,785
8080	Home Health Care Services	$5,656	$3,186
8090	Misc Health & And Allied Services	$3,649	$2,055
n/a	Fully Insured/ ERISA[3]	N/A	N/A
n/a	IRB[3]	N/A	N/A
n/a	Average for All Small Business	$4,188	$2,217

[1] Source: Office of Advocacy, U.S. Small Business Administration, from data provided by the Bureau of the Census, Statistics of U.S. Businesses, 1997. Entities that have less than $5,000,000 in annual revenue are considered small businesses here, as are non-profit entities (regardless of revenue). We have non-profit data for the following SICs: 8050, 8080, and 8060 and have included the number of non-profits in each category into the table.

[2] We have included self-insured/self-administered health plans and third party administrators in the total number of health plans, even though neither has individual SIC codes because we have the ability to impute revenues to them.

[2]We have not included the number of fully insured ERISA health plans or institutional review boards (IRB) in the total number of health care entities or the number of entities that meet SMA standards for small entities, since these are not separate businesses with SIC codes and we do not have sufficient data to impute revenues to them.

Table E shows the cost to each SIC code of the major cost items of the final rule. Listed are the top-five most costly provisions of the rule (to small business) and then the cost of all other remaining provisions. The costs of the most expensive five provisions represent 90 percent of the cost of the ongoing costs to small business, while the remaining provisions only represent 7 percent.

Table E.—Average Annual Ongoing Cost to Small Business of Implementing Provisions of the Privacy Regulation, After the First Year [1]

Industry	Average Annual Ongoing Cost for Privacy Official, per Industry Sector	Average Annual Ongoing Cost for Minimum Necessary, per Industry Sector	Average Annual Ongoing Cost for Disclosure Tracking, per Industry Sector	Average Annual Ongoing Cost for De-Identification, per Industry Sector	Average Annual Ongoing Cost for Training, per Industry Sector	Average Annual Ongoing Cost for All Other Provisions, per Industry Sector
Drug Stores & Proprietary Stores	$37,997,168	$30,008,085	$3,597,262	$3,751,011	$4,083,677	$7,293,227
Accident & Health Insurance & Medical Service plans (including Self Insured/ Self Administered Health plans, & TPAs)[2]	$5,920,267	$5,395,070	$985,072	$3,614,697	$59,086	$2,863,657
Medical Equipment Rental & Leasing	$1,769,789	$1,397,683	$167,549	$174,710	$190,205	$339,696
Offices & clinics of Doctors of Medicine	$156,215,538	$123,370,486	$14,789,213	$15,421,311	$16,788,984	$29,984,217

Offices & clinics of Doctors of Dentists	$70,027,863	$55,304,176	$6,629,667	$6,913,022	$7,526,119	$13,441,241
Offices & clinics of Doctors of Osteopathy	$5,991,323	$4,731,619	$567,210	$591,452	$643,907	$1,149,982
Offices & clinics of Other Health Practitioners	$34,363,581	$27,138,476	$3,253,264	$3,392,310	$3,693,164	$6,595,791
Nursing & Personal care Facilities	$36,311,120	$28,676,536	$3,437,641	$3,584,567	$3,902,472	$6,969,604
Hospitals	$25,475,393	$56,613,285	$19,558,912	$14,153,321	$309,555	$17,167,095
Medical & Dental Laboratories	$10,177,614	$8,037,723	$963,534	$1,004,715	$1,093,821	$1,953,505
Home Health care Services	$17,923,769	$14,155,212	$1,696,876	$1,769,402	$1,926,325	$3,440,312
Misc Health & Allied Health Services	$10,102,539	$7,978,433	$956,426	$997,304	$1,085,752	$1,939,095
Fully Insured/ERISA	N/A	N/A	N/A	N/A	N/A	$9,351,383
IRB	N/A	N/A	N/A	N/A	N/A	$0
Total	$412,275,964	$362,806,784	$56,602,625	$55,367,822	$41,303,067	$102,488,804

[1] Source: Office of Advocacy, U.S. Small Business Administration, from data provided by the Bureau of the Census, Statistics of U.S. Businesses, 1997. Entities that have less than $5,000,000 in annual revenue are considered small businesses here, as are

[2] We have included self-insured, self-administered health plans and third party administrators in the total number of health plans, even though neither has individual SIC codes because we have the ability to impute revenues to them.

VI. Unfunded Mandates

The Unfunded Mandates Reform Act of 1995 (Pub. L. 104–4) requires cost-benefit and other analyses for rules that would cost more than $100 million in a single year. The rule qualifies as a significant rule under the statute. The Department has carried out the cost-benefit analysis in sections D and E of this document, which includes a discussion of unfunded costs to state and local governments resulting from this regulation. In developing this regulation, the Department adopted the least burdensome alternatives, consistent with achieving the rule's goals.

A. Future Costs

The Department estimates some of the future costs of the rule in Section E of the Preliminary Regulatory Impact Analysis of this document. The estimates made include costs for the ten years after the effective date. As discussed in section E, state and local government costs will be in the order of $460 million in 2003 and $2.4 billion over ten years. Estimates for later years are not practical. The changes in technology are likely to alter the nature of medical record-keeping, and the uses of medical data are likely to vary dramatically over this period. Therefore, any estimates for years beyond 2012 are not feasible.

B. Particular Regions, Communities, or Industrial Sectors

The rule applies to the health care industry and would, therefore, affect that industry disproportionately. Any long-run increase in the costs of health care services would largely be passed on to the entire population of consumers. However, as discussed in the administrative implication regulation, the Transactions Rule is estimated to save the health care industry nearly $30 billion over essentially the same time period. This more than offsets the costs of the Privacy Rule; indeed, as discussed above, the establishment of consistent, national standards for the protection of medical information is essential to fully realize the savings from electronic transactions standards and other advances that may be realized through ''e-health'' over the next decade. Without strong privacy rules, patients and providers may be very reluctant to fully participate in electronic and e-health opportunities.

C. National Productivity and Economic Growth

The rule is not expected to substantially affect productivity or economic growth. It is possible that productivity and growth in certain sectors of the health care industry could be slightly lower than otherwise because of the need to divert research and development resources to compliance activities. The diversion of resources to compliance activities would be temporary. Moreover, the Department anticipates that, because the benefits of privacy are large, both productivity and economic growth would be higher than in the absence of the final rule. In section I.A. of this document, the Department discusses its expectation that this rule will increase communication among consumers, health plans, and providers and that implementation of privacy protections will lead more people to seek health care. The increased health of the population will lead to increased productivity and economic growth.

D. Full Employment and Job Creation

Some of the human resources devoted to the delivery of health care services will be redirected by rule. The rule could lead to some short-run changes in employment patterns as a result of the structural changes within the health care industry. The growth of employment (job creation) for the roles typically associated with health care profession could also temporarily change but be balanced by an increased need for those who can assist entities with complying with this rule. Therefore, while there could be a temporary slowing of growth in traditional health care professions, that will be offset by a temporary increase in growth in fields that may assist with compliance with this rule (*e.g.* worker training, and management consultants).

E. Exports

Because the rule does not mandate any changes in products, current export products will not be required to change in any way.

The Department consulted with state and local governments, and Tribal governments. See sections X and XI, below.

VII. Environmental Impact

The Department has determined under 21 CFR 25.30(k) that this action is of a type of does not individually or cumulatively have a significant effect on the human environment. Therefore, neither an environmental assessment nor an environmental impact statement is required.

VIII. Collection of Information Requirements

Under the Paperwork Reduction Act of 1995 PRA), agencies are required to provide a 30-day notice in the **Federal Register** and solicit public comment before a collection of information requirement is submitted to the Office of Management and Budget (OMB) for review and approval. In order to fairly evaluate whether an information collection should be approved by OMB, section 3506(c)(2)(A) of the PRA requires that we solicit comment on the following issues:

- Whether the information collection is necessary and useful to carry out the proper functions of the agency;
- The accuracy of the agency's estimate of the information collection burden;
- The quality, utility, and clarity of the information to be collected; and
- Recommendations to minimize the information collection burden on the affected public, including automated collection techniques.

Under the PRA, the time, effort, and financial resources necessary to meet the information collection requirements referenced in this section are to be considered. Due to the complexity of this regulation, and to avoid redundancy of effort, we are referring readers to Section V (Final Regulatory Impact Analysis) above, to review the detailed cost assumptions associated with these PRA requirements. We explicitly seek, and will consider, public comment on our assumptions as they relate to the PRA requirements summarized in this section.

Section 160.204—Process for Requesting Exception Determinations

Section 160.204 would require persons requesting to except a provision of state law from preemption under § 160.203(a) to submit a written request, that meets the requirements of this section, to the Secretary to except a provision of state law from preemption under § 160.203. The burden associated with these requirements is the time and effort necessary for a state to prepare and submit the written request for an exception determination to the Secretary for approval. On an annual basis it is estimated that it will take 40 states 16 hours each to prepare and submit a request. The total annual burden associated with this requirement is 640 hours. The Department solicits public comment on the number of requests and hours for others likely to submit requests.

Section 160.306—Complaints to the Secretary

A person who believes that a covered entity is not complying with the applicable requirements of part 160 or the applicable standards, requirements,

and implementation specifications of Subpart E of part 164 of this subchapter may file a complaint with the Secretary. This requirement is exempt from the PRA as stipulated under 5 CFR 1320.4(a)(2), an audit/administrative action exemption.

Section 160.310—Responsibilities of Covered Entities

A covered entity must keep such records and submit such compliance reports, in such time and manner and containing such information, necessary to enable the Secretary to ascertain whether the covered entity has complied or is complying with the applicable requirements of part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164. Refer to § 164.530 for discussion.

Section 164.502—Uses and Disclosures of Protected Health Information: General Rules

A covered entity is permitted to disclose protected health information to an individual, and is required to provide and individual with access to protected health information, in accordance with the requirements set forth under § 164.524. Refer to § 164.524 for discussion.

Section 164.504—Uses and Disclosures—Organizational Requirements

Except for disclosures of protected health information by a covered entity that is a health care provider to another health care provider for treatment purposes, § 164.504 requires a covered entity to maintain documentation demonstrating that it meets the requirements set forth in this section and to demonstrate that it has obtained satisfactory assurance from business associates that meet the requirements of this part with each of its business associates. The burden is 5 minutes per entity times an annual average of 764,799 entities for a total burden of 63,733 burden hours.

Section 164.506—Consent for Treatment, Payment, and Health Care Operations

Except in certain circumstances, a covered health care provider that has a direct treatment relationship must obtain an individual's consent for use or disclosure of protected health information for treatment, payment, or health care operations. While this requirement is subject to the PRA, we believe that the burden associated with this requirement is exempt from the PRA as stipulated under 5 CFR 1320.3(b)(2).

Section 164.508—Uses and Disclosures for Which Individual Authorization Is Required

Under this section, a covered entity will need to obtain a written authorization from an individual, before it uses or discloses protected health information of the individual if the use or disclosure is not otherwise permitted or required under the rule without authorization. The burden associated with these requirements is the time and effort necessary for a covered entity to obtain written authorization prior to the disclosure of individually identifiable health information. On an annual basis, we estimate that it will take 764,799 entities, an annual average burden per entity of one hour for a total annual burden of 764,799 burden hours.

Section 164.510—Uses and Disclosures Requiring an Opportunity for the Individual To Agree or To Object

Section 164.510 allows, but does not require, covered entities to use or disclose protected health information: (1) for health care institutions, directories; and (2) to family members, close friends, or other persons assisting in an individual's care, as well as government agencies and disaster relief organizations conducting disaster relief activities. This section of the rule addresses situations in which the interaction between the covered entity and the individual is relatively informal, and agreements may be made orally, without written authorizations for use or disclosure. In general, to disclose protected health information for these purposes, covered entities must inform individuals in advance and must provide a meaningful opportunity for the individual to prevent or restrict the disclosure. In certain circumstances, such as in an emergency, when this informal discussion cannot practicably occur, covered entities can make decisions about disclosure or use, in accordance with the requirements of this section based on their professional judgment of what is in the patient's best interest. While these provisions are subject to the PRA, we believe that the burden associated with this requirement is exempt from the PRA as stipulated under 5 CFR 1320.3(b)(2).

Section 164.512—Uses and Disclosures for Which Consent, Individual Authorization, or Opportunity To Agree or Object Is Not Required

Section 164.1512 includes provisions that allow, but that do not require, covered entities to disclose protected health information without individual authorization for a variety of purposes which represent important national priorities. Pursuant to § 164.512, covered entities may disclose protected health information for specified purposes as follows: as required by law; for public health activities; to public officials regarding victims of abuse, neglect, or domestic violence; for health oversight; for judicial and administrative proceedings; for law enforcement; for specified purposes regarding decedents; for organ donation and transplantation; for research; to avert an imminent threat to health or safety; for specialized government functions (such as for intelligence and national security activities); and to comply with workers' compensation laws. While these provisions are subject to the PRA, we believe that the burden associated with this requirement is exempt from the PRA as stipulated under 5 CFR 1320.3(b)(2).

For research, if a covered entity wants to use or disclose protected health information without individual authorization, it must obtain documentation that a waiver, in whole or in part, of the individual authorization required by § 164.508 for use or disclosure of protected health information has been approved by either an Institutional Review Board (IRB), established in accordance with 7 CFR 1c.107, 10 CFR 745.107, 14 CFR 1230.107, 15 CFR 27.107, 16 CFR 1028.107, 21 CFR 56.107, 22 CFR 225.107, 28 CFR 46.107, 32 CFR 219.107, 34 CFR 97.107, 38 CFR 16.107, 40 CFR 26.107, 45 CFR 46.107, 45 CFR 690.107, or 49 CFR 11.107; or a privacy board. The burden associated with these requirements is the time and effort necessary for a covered entity to maintain documentation demonstrating that they have obtained IRB or privacy board approval, which meet the requirements of this section. On an annual basis it is estimated that these requirements will affect 113,524 IRB reviews. We further estimate that it will take an average of 5 minutes per review to meet these requirements on an annual basis. Therefore, the total estimated annual burden associated with this requirement is 9,460 hours.

Section 164.514—Other Procedural Requirements Relating to Uses and Disclosures of Protected Health Information

Prior to any disclosure permitted by this subpart, a covered entity must verify the identity and authority of persons requesting protected health information, if the identity or authority of such person is not known to the

covered entity, and obtain any documentation, statements, or representations from the person requesting the protected health information that is required as a condition of the disclosure. In addition, a covered entity must retain any signed consent pursuant to § 164.506 and any signed authorization pursuant to § 164.508 for documentation purposes as required by § 164.530(j). This requirement is exempt from the PRA as stipulated under 5 CFR 1320.4(a)(1) and (1)(2).

Section 164.520—Notice of Privacy Practices for Protected Health Information

Except in certain circumstances set forth in this section, individuals have a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information. To comply with this requirement a covered entity must provide a notice, written in plain language, that includes the elements set forth in this section. For health plans, there will be an average of 160.2 million notices each year. We assume that the most efficient means of distribution for health plans will be to send them out annually as part of the materials they send to current and potential enrollees, even though it is not required by the regulation. The number of notices per health plan per year would be about 10,570. We further estimate that it will require each health plan, on average, only 10 seconds to disseminate each notice. The total annual burden associated with this requirement is calculated to be 267,000 hours. Health care providers with direct treatment relationships would provide a copy of the notice to an individual at the time of first service delivery to the individual, make the notice available at the service delivery site for individuals to request and take with them, whenever the content of the notice is revised, make the notice available upon request and post the notice, if required by this section, and post a copy of the notice in a location where it is reasonable to expect individuals seeking services from the provider to be able to read the notice. The annual number of notices disseminated by all providers is 613 million. We further estimate that it will require each health provider, on average, 10 seconds to disseminate each notice. This estimate is based upon the assumption that the required notice will be incorporated into and disseminated with other patient materials. The total annual burden associated with this requirement is calculated to be 1 million hours.

In addition, a covered entity must document compliance with the notice requirements by retaining copies of the notices issued by the covered entity. Refer to § 164.530 for discussion.

Section 164.522—Rights To Request Privacy Proteciton for Protected Health Information

Given that the burden associated with the following information collection requirements will differ significantly, by the type and size of health plan or health care provider, we are explicitly soliciting comment on the burden associated with the following requirements; as outlined and required by this section, covered entities must provide individuals with the opportunity to request restrictions related to the uses or disclosures of protected health information for treatment, payment, or health care operations. In addition, covered entities must accommodate requests for confidential communications in certain situations.

Section 164.524—Access of Individuals to Protected Health Information

As set forth in this section, covered entities must provide individuals with access to inspect and obtain a copy of protected health information about them in designated record sets, for so long as the protected health information is maintained in the designated record sets. This includes such information in a business associate's designated record set that is not a duplicate of the information held by the health care provider or health plan for so long as the information is maintained. Where the request is denied in whole or in part, the covered entity must provide the individual with a written statement of the basis for the denial and a description of how the individual may complain to the covered entity pursuant to the complaint procedures established in § 164.530 or to the Secretary pursuant to the procedures established in § 160.306 of this subpart. In certain cases, the covered entity must provide the individual the opportunity to have another health care professional review the denial. Pursuant to public comment, we estimate that each disclosure will contain 31 pages and that 150,000 disclosures will be made on an annual basis at three minutes per disclosure for a total burden of 7,500 hours. Refer to section V.E. for detailed discussion related to the costs associated with meeting these requirements.

Section 164.526—Amendment of Protected Health Information

Given that burden associated with the following information collection requirements will differ significantly, by the type and size of health plan or health care provider, we are explicitly soliciting comment on the burden associated with the following requirements: Individuals have the right to request amendment of protected health information about them in designated record sets created by a covered entity. Where the request is denied, a covered entity must provide the individual with a written statement of the basis for the denial and an explanation of how the individual may pursue the matter, including how to file a complaint with the Secretary pursuant to § 160.306 of this subpart. As appropriate, a covered entity must identify the protected health information in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the covered entity's denial of the request, the individual's statement of disagreement, if any, and the covered entity's rebuttal, if any, to the designated record set.

Section 164.528—Accounting for Disclosures of Protected Health Information

Based upon public comment it is assumed that it will take 5 minutes per request times 1,081,000 requests for an annual burden of 90,083 hours. An individual may request that a covered entity provide an accounting for disclosure for a period of time less than six years from the date of the individual's request, as outlined in this section.

Section 164.530—Administrative Requirements

A covered entity must maintain such policies and procedures in written or electronic form where policies or procedures with respect to protected health information are required by this subpart. Where a communication is required by this subpart to be in writing, a covered entity must maintain such writing, or an electronic copy, as documentation; and where an action or activity is required by this subpart to be documented, it must maintain a written or electronic record of such action or activity. While these requirements are subject to the PRA, we believe the burden associated with these requirements is exempt from the PRA as stipulated under 5 CFR 1320.3(b)(2).

We have submitted a copy of this rule to OMB for its review of the information collection requirements in §§ 160.204, 160.306, 160.310, 164.502, 164.504, 164.506, 164.508, 164.510, 164.512, 164.514, 164.520, 164.522, 164.524, 164.526, 164.528, and Sec. 164.530. These requirements are not effective until they have been approved by OMB. If you comment on any of these information collection and record keeping requirements, please mail copies directly to the following: Health Care Financing Administration, Office of Information Services, Division of HCFA Enterprise Standards, Room N2–14–26, 7500 Security Boulevard, Baltimore, MD 21244–1850. ATTN: John Burke and to the Office of Information and Regulatory Affairs, Office of Management and Budget, Room 10235, New Executive Office Building, Washington, DC 20503. ATTN: Allison Herron Eydt, HCFA Desk Officer.

IX. Executive Order 13132: Federalism

The Department has examined the effects of provisions in the final privacy regulation on the relationship between the federal government and the states, as required by Executive Order 13132 on ''Federalism.'' Our conclusion is that the final rule does have federalism implications because the rule has substantial direct effects on states, on the relationship between the national government and states, and on the distribution of power and responsibilities among the various levels of government. The federalism implications of the rule, however, flow from, and are consistent with the underlying statute. The statute allows us to preempt state or local rules that provide less stringent privacy protection requirements than federal law is consistent with this Executive Order. Overall, the final rule attempts to balance both the autonomy of the states with the necessity to create a federal benchmark to preserve the privacy of personally identifiable health information.

It is recognized that the states generally have laws that relate to the privacy of individually identifiable health information. The HIPAA statue dictates the relationship between state law and this final rule. Except for laws that are specifically exempted by the HIPAA statute, state laws continue to be enforceable, unless they are contrary to Part C of Title XI of the standards, requirements, or implementation specifications adopted or pursuant to subpart x. However, under section 264(c)(2), not all contrary provisions of state privacy laws are preempted; rather, the law provides that contrary provisions of state law relating to the privacy of individually identifiable health information that are also ''more stringent'' than the federal regulatory requirements or implementation specifications will continue to be enforceable.

Section 3(b) of Executive Order 13132 recognizes that national action limiting the policymaking discretion of states will be imposed ''* * * only where there is constitutional and statutory authority for the action and the national activity is appropriate in light of the presence of a problem of national significance.'' Personal privacy issues are widely identified as a national concern by virtue of the scope of interstate health commerce. HIPAA's provisions reflect this position. HIPAA attempts to facilitate the electronic exchange of financial and administrative health plan transactions while recognizing challenges that local, national, and international information sharing raise to confidentiality and privacy of health information.

Section 3(d)(2) of the Executive Order 13132 requires the federal government defer to the states to establish standards where possible. HIPAA requires the Department to establish standards, and we have done so accordingly. This approach is a key component of the final Privacy Rule, and it adheres to section 4(a) of Executive Order 13132, which expressly contemplates preemption when there is a conflict between exercising state and federal authority under federal statute. Section 262 of HIPAA enacted Section 1178 of the Social Security Act, developing a ''general rule'' that state laws or provisions that are contrary to the provisions or requirements of Part C of Title XI, or the standards or implementation specifications adopted, or established thereunder are preempted. Several exceptions to this rule exist, each of which is designed to maintain a high degree of state autonomy.

Moreover, section 4(b) of the Executive Order authorizes preemption of state law in the federal rule making context when there is ''the exercise of state authority is directly conflicts with the exercise of federal authority under federal statute * * *.'' Section 1178 (a)(2)(B) of HIPAA specifically preempts state laws related to the privacy of individually identifiable health information unless the state law is more stringent. Thus, we have interpreted state and local laws and regulations that would impose less stringent requirements for protection of individually identifiable health information as undermining the agency's goal of ensuring that all patients who receive medical services are assured a minimum level of personal privacy. Particularly where the absence of privacy protection undermines an individual's access to health care services, both the personal and public interest is served by establishing federal rules.

The final rule would establish national minimum standards with respect to the collection, maintenance, access, use, and disclosure of individually identifiable health information. The federal law will preempt state law only where state and federal laws are ''contradictory'' and the federal regulation is judged to establish ''more stringent'' privacy protections than state laws.

As required by the previous Executive Order (E.O. 13132), states and local governments were given, through the notice of proposed rule making, an opportunity to participate in the proceedings to preempt state and local laws (section 4(e)). The Secretary also provided a review of preemption issues upon requests from states. In addition, anticipating the promulgation of the Executive Order, appropriate officials and organizations were consulted before this proposed action is implemented (Section 3(a) of Executive Order 13132).

The same section also includes some qualitative discussion of costs that would occur beyond that time period. Most of the costs of proposed rule, however, would occur in the years immediately after the publication of a final rule. Future costs beyond the ten year period will continue but will not be as great as the initial compliance costs.

Finally, we have considered the cost burden that this proposed rule would impose on state and local health care programs, such as Medicaid, county hospitals, and other state health benefits programs. As discussed in Section E of the Regulatory Impact Analysis of this document, we estimate state and local government costs will be in the order of $460 million in 2003 and $2.4 billion over ten years.

The agency concludes that the policy in this final document has been assessed in light of the principles, criteria, and requirements in Executive Order 13132; that this policy is not inconsistent with that Order; that this policy will not impose significant additional costs and burdens on the states; and that this policy will not affect the ability of the states to discharge traditional state governmental functions.

During our consultation with the states, representatives from various state agencies and offices expressed concern that the final regulation would preempt

all state privacy laws. As explained in this section, the regulation would only preempt state laws where there is a direct conflict between state laws and the regulation, and where the regulation provides more stringent privacy protection than state law. We discussed this issue during our consultation with state representatives, who generally accepted our approach to the preemption issue. During the consultation, we requested further information from the states about whether they currently have laws requiring that providers have a ''duty to warn'' family members or third parties about a patient's condition other than in emergency circumstances. Since the consultation, we have not received additional comments or questions from the states.

X. Executive Order 13086; Consultation and Coordination With Indian Tribal Governments

In drafting the proposed rule, the Department consulted with representatives of the National Congress of American Indians and the National Indian Health Board, as well as with a representative of the self-governance Tribes. During the consultation, we discussed issues regarding the application of Title II of HIPAA to the Tribes, and potential variations based on the relationship of each Tribe with the IHS for the purpose of providing health services. Participants raised questions about the status of Tribal laws regarding the privacy of health information.

List of Subjects

45 CFR Part 160

Electronic transactions, Employer benefit plan, Health, Health care, Health facilities, Health insurance, Health records, Medicaid, Medical research, Medicare, Privacy, Reporting and record keeping requirements.

45 CFR Part 164

Electronic transactions, Employer benefit plan, Health, Health care, Health facilities, Health insurance, Health records, Medicaid, Medical research, Medicare, Privacy, Reporting and record keeping requirements.

Note: to reader: This final rule is one of several proposed and final rules that are being published to implement the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996. 45 CFR subchapter C consisting of Parts 160 and 162 was added at 65 FR 50365, Aug. 17, 2000. Part 160 consists of general provisions, Part 162 consists of the various administrative simplification regulations relating to transactions and identifiers, and new Part 164 consists of the regulations implementing the security and privacy requirements of the legislation.

Dated: December 19, 2000.

Donna Shalala,

Secretary,

For the reasons set forth in the preamble, 45 CFR Subtitle A, Subchapter C, is amended as follows:

1. Part 160 is revised to read as follows:

PART 160—GENERAL ADMINISTRATIVE REQUIREMENTS

Subpart A—General Provisions

Subpart B—Preemption of State Law

Subpart C—Compliance and Enforcement

Authority: Sec. 1171 through 1179 of the Social Security Act, (42 U.S.C. 1320d–1329d–8) as added by sec. 262 of Pub. L. 104–191, 110 Stat. 2021–2031 and sec. 264 of Pub. L. 104–191 (42 U.S.C. 1320d–2(note)).

Subpart A—General Provisions

§ 160.101 Statutory basis and purpose.

The requirements of this subchapter implement sections 1171 through 1179 of the Social Security Act (the Act), as added by section 262 of Public Law 104–191, and section 264 of Public Law 104–191.

§ 160.102 Applicability.

(a) Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to the following entities:

(1) A health plan.

(2) A health care clearinghouse.

(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

(b) To the extent required under section 201(a)(5) of the Health Insurance Portability Act of 1996, (Pub. L. 104–191), nothing in this subchapter shall be construed to diminish the authority of any Inspector General, including such authority as provided in the Inspector General Act of 1978, as amended (5 U.S.C. App.).

§ 160.103 Definitions.

Except as otherwise provided, the following definitions apply to this subchapter:

Act means the Social Security Act.

ANSI stands for the American National Standards Institute.

Business associate: (1) Except as provided in paragraph (2) of this definition, *business associate* means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in § 164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:

(A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or

(B) Any other function or activity regulated by this subchapter; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service,

become a business associate of other covered entities participating in such organized health care arrangement.

(3) A covered entity may be a business associate of another covered entity.

Compliance date means the date by which a covered entity must comply with a standard, implementation specification, requirement, or modification adopted under this subchapter.

Covered entity means:

(1) A health plan.

(2) A health care clearinghouse.

(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

Group health plan (also see definition of *health plan* in this section) means an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act (PHS Act), 42 U.S.C. 300gg–91(a)(2)), including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that:

(1) Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7)); or

(2) Is administered by an entity other than the employer that established and maintains the plan.

HCFA stands for Health Care Financing Administration within the Department of Health and Human Services.

HHS stands for the Department of Health and Human Services.

Health care means care, services, or supplies related to the health of an individual. *Health care* includes, but is not limited to, the following:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and

(2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health care clearinghouse means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and ''value-added'' networks and switches, that does either of the following functions:

(1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

(2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health care provider means a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health information means any information, whether oral or recorded in any form or medium, that:

(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Health insurance issuer (as defined in section 2791(b)(2) of the PHS Act, 42 U.S.C. 300gg–91(b)(2) and used in the definition of *health plan* in this section) means an insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance. Such term does not include a group health plan.

Health maintenance organization (HMO) (as defined in section 2791(b)(3) of the PHS Act, 42 U.S.C. 300gg–91(b)(3) and used in the definition of *health plan* in this section) means a federally qualified HMO, an organization recognized as an HMO under State law, or a similar organization regulated for solvency under State law in the same manner and to the same extent as such an HMO.

Health plan means an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg–91(a)(2)).

(1) *Health plan* includes the following, singly or in combination:

(i) A group health plan, as defined in this section.

(ii) A health insurance issuer, as defined in this section.

(iii) An HMO, as defined in this section.

(iv) Part A or Part B of the Medicare program under title XVIII of the Act.

(v) The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, *et seq.*

(vi) An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)).

(vii) An issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy.

(viii) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.

(ix) The health care program for active military personnel under title 10 of the United States Code.

(x) The veterans health care program under 38 U.S.C. chapter 17.

(xi) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) (as defined in 10 U.S.C. 1072(4)).

(xii) The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, *et seq.*

(xiii) The Federal Employees Health Benefits Program under 5 U.S.C. 8902, *et seq.*

(xiv) An approved State child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, *et seq.*

(xv) The Medicare+Choice program under Part C of title XVIII of the Act, 42 U.S.C. 1395w–21 through 1395w–28.

(xvi) A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals.

(xvii) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg–91(a)(2)).

(2) *Health plan* excludes:

(i) Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg–91(c)(1); and

(ii) A government-funded program (other than one listed in paragraph (1)(i)–(xvi) of this definition):

(A) Whose principal purpose is other than providing, or paying the cost of, health care; or

(B) Whose principal activity is:

(1) The direct provision of health care to persons; or

(2) The making of grants to fund the direct provision of health care to persons.

Implementation specification means specific requirements or instructions for implementing a standard.

Modify or *modification* refers to a change adopted by the Secretary, through regulation, to a standard or an implementation specification.

Secretary means the Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.

Small health plan means a health plan with annual receipts of $5 million or less.

Standard means a rule, condition, or requirement:

(1) Describing the following information for products, systems, services or practices:

(i) Classification of components.

(ii) Specification of materials, performance, or operations; or

(iii) Delineation of procedures; or

(2) With respect to the privacy of individually identifiable health information.

Standard setting organization (SSO) means an organization accredited by the American National Standards Institute that develops and maintains standards for information transactions or data elements, or any other standard that is necessary for, or will facilitate the implementation of, this part.

State refers to one of the following:

(1) For a health plan established or regulated by Federal law, State has the meaning set forth in the applicable section of the United States Code for such health plan.

(2) For all other purposes, *State* means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam.

Trading partner agreement means an agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or part of a larger agreement, between each party to the agreement. (For example, a trading partner agreement may specify, among other things, the duties and responsibilities of each party to the agreement in conducting a standard transaction.)

Transaction means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

(1) Health care claims or equivalent encounter information.

(2) Health care payment and remittance advice.

(3) Coordination of benefits.

(4) Health care claim status.

(5) Enrollment and disenrollment in a health plan.

(6) Eligibility for a health plan.

(7) Health plan premium payments.

(8) Referral certification and authorization.

(9) First report of injury.

(10) Health claims attachments.

(11) Other transactions that the Secretary may prescribe by regulation.

Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

§ 160.104 Modifications.

(a) Except as provided in paragraph (b) of this section, the Secretary may adopt a modification to a standard or implementation specification adopted under this subchapter no more frequently than once every 12 months.

(b) The Secretary may adopt a modification at any time during the first year after the standard or implementation specification is initially adopted, if the Secretary determines that the modification is necessary to permit compliance with the standard or implementation specification.

(c) The Secretary will establish the compliance date for any standard or implementation specification modified under this section.

(1) The compliance date for a modification is no earlier than 180 days after the effective date of the final rule in which the Secretary adopts the modification.

(2) The Secretary may consider the extent of the modification and the time needed to comply with the modification in determining the compliance date for the modification.

(3) The Secretary may extend the compliance date for small health plans, as the Secretary determines is appropriate.

Subpart B—Preemption of State Law

§ 160.201 Applicability.

The provisions of this subpart implement section 1178 of the Act, as added by section 262 of Public Law 104–191.

§ 160.202 Definitions.

For purposes of this subpart, the following terms have the following meanings:

Contrary, when used to compare a provision of State law to a standard, requirement, or implementation specification adopted under this subchapter, means:

(1) A covered entity would find it impossible to comply with both the State and federal requirements; or

(2) The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act or section 264 of Pub. L. 104–191, as applicable.

More stringent means, in the context of a comparison of a provision of State law and a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter, a State law that meets one or more of the following criteria:

(1) With respect to a use or disclosure, the law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted under this subchapter, except if the disclosure is:

(i) Required by the Secretary in connection with determining whether a covered entity is in compliance with this subchapter; or

(ii) To the individual who is the subject of the individually identifiable health information.

(2) With respect to the rights of an individual who is the subject of the individually identifiable health information of access to or amendment of individually identifiable health information, permits greater rights of access or amendment, as applicable; provided that, nothing in this subchapter may be construed to preempt any State law to the extent that it authorizes or prohibits disclosure of protected health information about a minor to a parent, guardian, or person acting *in loco parentis* of such minor.

(3) With respect to information to be provided to an individual who is the subject of the individually identifiable health information about a use, a disclosure, rights, and remedies, provides the greater amount of information.

(4) With respect to the form or substance of an authorization or consent for use or disclosure of individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the authorization or consent, as applicable.

(5) With respect to recordkeeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information or for a longer duration.

(6) With respect to any other matter, provides greater privacy protection for the individual who is the subject of the individually identifiable health information.

Relates to the privacy of individually identifiable health information means, with respect to a State law, that the State law has the specific purpose of protecting the privacy of health information or affects the privacy of health information in a direct, clear, and substantial way.

State law means a constitution, statute, regulation, rule, common law, or other State action having the force and effect of law.

§ 160.203 General rule and exceptions.

A standard, requirement, or implementation specification adopted under this subchapter that is contrary to a provision of State law preempts the provision of State law. This general rule applies, except if one or more of the following conditions is met:

(a) A determination is made by the Secretary under § 160.204 that the provision of State law:

(1) Is necessary:

(i) To prevent fraud and abuse related to the provision of or payment for health care;

(ii) To ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation;

(iii) For State reporting on health care delivery or costs; or

(iv) For purposes of serving a compelling need related to public health, safety, or welfare, and, if a standard, requirement, or implementation specification under part 164 of this subchapter is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or

(2) Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances (as defined in 21 U.S.C. 802), or that is deemed a controlled substance by State law.

(b) The provision of State law relates to the privacy of health information and is more stringent than a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter.

(c) The provision of State law, including State procedures established under such law, as applicable, provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention.

(d) The provision of State law requires a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals.

§ 160.204 Process for requesting exception determinations.

(a) A request to except a provision of State law from preemption under § 160.203(a) may be submitted to the Secretary. A request by a State must be submitted through its chief elected official, or his or her designee. The request must be in writing and include the following information:

(1) The State law for which the exception is requested;

(2) The particular standard, requirement, or implementation specification for which the exception is requested;

(3) The part of the standard or other provision that will not be implemented based on the exception or the additional data to be collected based on the exception, as appropriate;

(4) How health care providers, health plans, and other entities would be affected by the exception;

(5) The reasons why the State law should not be preempted by the federal standard, requirement, or implementation specification, including how the State law meets one or more of the criteria at § 160.203(a); and

(6) Any other information the Secretary may request in order to make the determination.

(b) Requests for exception under this section must be submitted to the Secretary at an address that will be published in the **Federal Register**. Until the Secretary's determination is made, the standard, requirement, or implementation specification under this subchapter remains in effect.

(c) The Secretary's determination under this section will be made on the basis of the extent to which the information provided and other factors demonstrate that one or more of the criteria at § 160.203(a) has been met.

§ 160.205 Duration of effectiveness of exception determinations.

An exception granted under this subpart remains in effect until:

(a) Either the State law or the federal standard, requirement, or implementation specification that provided the basis for the exception is materially changed such that the ground for the exception no longer exists; or

(b) The Secretary revokes the exception, based on a determination that the ground supporting the need for the exception no longer exists.

Subpart C—Compliance and Enforcement

§ 160.300 Applicability.

This subpart applies to actions by the Secretary, covered entities, and others with respect to ascertaining the compliance by covered entities with and the enforcement of the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

§ 160.302 Definitions.

As used in this subpart, terms defined in § 164.501 of this subchapter have the same meanings given to them in that section.

§ 160.304 Principles for achieving compliance.

(a) *Cooperation.* The Secretary will, to the extent practicable, seek the cooperation of covered entities in obtaining compliance with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

(b) *Assistance.* The Secretary may provide technical assistance to covered entities to help them comply voluntarily with the applicable requirements of this part 160 or the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

§ 160.306 Complaints to the Secretary.

(a) *Right to file a complaint.* A person who believes a covered entity is not complying with the applicable requirements of this part 160 or the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter may file a complaint with the Secretary.

(b) *Requirements for filing complaints.* Complaints under this section must meet the following requirements:

(1) A complaint must be filed in writing, either on paper or electronically.

(2) A complaint must name the entity that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable requirements of this part 160 or the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

(3) A complaint must be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred, unless this time limit is waived by the Secretary for good cause shown.

(4) The Secretary may prescribe additional procedures for the filing of complaints, as well as the place and manner of filing, by notice in the **Federal Register**.

(c) *Investigation.* The Secretary may investigate complaints filed under this section. Such investigation may include a review of the pertinent policies, procedures, or practices of the covered entity and of the circumstances regarding any alleged acts or omissions concerning compliance.

§ 160.308 Compliance reviews.

The Secretary may conduct compliance reviews to determine whether covered entities are complying with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

§ 160.310 Responsibilities of covered entities.

(a) *Provide records and compliance reports.* A covered entity must keep such records and submit such compliance reports, in such time and manner and containing such information, as the Secretary may determine to be necessary to enable the Secretary to ascertain whether the covered entity has complied or is complying with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

(b) *Cooperate with complaint investigations and compliance reviews.* A covered entity must cooperate with the Secretary, if the Secretary undertakes an investigation or compliance review of the policies, procedures, or practices of a covered entity to determine whether it is complying with the applicable requirements of this part 160 and the standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

(c) *Permit access to information.* (1) A covered entity must permit access by the Secretary during normal business hours to its facilities, books, records, accounts, and other sources of information, including protected health information, that are pertinent to ascertaining compliance with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter. If the Secretary determines that exigent circumstances exist, such as when documents may be hidden or destroyed, a covered entity must permit access by the Secretary at any time and without notice.

(2) If any information required of a covered entity under this section is in the exclusive possession of any other agency, institution, or person and the other agency, institution, or person fails or refuses to furnish the information, the covered entity must so certify and set forth what efforts it has made to obtain the information.

(3) Protected health information obtained by the Secretary in connection with an investigation or compliance review under this subpart will not be disclosed by the Secretary, except if necessary for ascertaining or enforcing compliance with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter, or if otherwise required by law.

§ 160.312 Secretarial action regarding complaints and compliance reviews.

(a) *Resolution where noncompliance is indicated.* (1) If an investigation pursuant to § 160.306 or a compliance review pursuant to § 160.308 indicates a failure to comply, the Secretary will so inform the covered entity and, if the matter arose from a complaint, the complainant, in writing and attempt to resolve the matter by informal means whenever possible.

(2) If the Secretary finds the covered entity is not in compliance and determines that the matter cannot be resolved by informal means, the Secretary may issue to the covered entity and, if the matter arose from a complaint, to the complainant written findings documenting the non-compliance.

(b) *Resolution when no violation is found.* If, after an investigation or compliance review, the Secretary determines that further action is not warranted, the Secretary will so inform the covered entity and, if the matter arose from a complaint, the complainant in writing.

2. A new Part 164 is added to read as follows:

PART 164—SECURITY AND PRIVACY

Subpart A—General Provisions

Sec.

Subparts B–D—[Reserved]

Subpart E—Privacy of Individually Identifiable Health Information

Authority: 42 U.S.C. 1320d–2 and 1320d–4, sec. 264 of Pub. L. 104–191, 110 Stat. 2033–2034 (42 U.S.C. 1320(d–2(note)).

Subpart A—General Provisions

§ 164.102 Statutory basis.

The provisions of this part are adopted pursuant to the Secretary's authority to prescribe standards, requirements, and implementation standards under part C of title XI of the Act and section 264 of Public Law 104–191.

§ 164.104 Applicability.

Except as otherwise provided, the provisions of this part apply to covered entities: health plans, health care clearinghouses, and health care providers who transmit health information in electronic form in connection with any transaction referred to in section 1173(a)(1) of the Act.

§ 164.106 Relationship to other parts.

In complying with the requirements of this part, covered entities are required to comply with the applicable provisions of parts 160 and 162 of this subchapter.

Subpart B–D—[Reserved]

Subpart E—Privacy of Individually Identifiable Health Information

§ 164.500 Applicability.

(a) Except as otherwise provided herein, the standards, requirements, and

implementation specifications of this subpart apply to covered entities with respect to protected health information.

(b) Health care clearinghouses must comply with the standards, requirements, and implementation specifications as follows:

(1) When a health care clearinghouse creates or receives protected health information as a business associate of another covered entity, the clearinghouse must comply with:

(i) Section 164.500 relating to applicability;

(ii) Section 164.501 relating to definitions;

(iii) Section 164.502 relating to uses and disclosures of protected health information, except that a clearinghouse is prohibited from using or disclosing protected health information other than as permitted in the business associate contract under which it created or received the protected health information;

(iv) Section 164.504 relating to the organizational requirements for covered entities, including the designation of health care components of a covered entity;

(v) Section 164.512 relating to uses and disclosures for which consent, individual authorization or an opportunity to agree or object is not required, except that a clearinghouse is prohibited from using or disclosing protected health information other than as permitted in the business associate contract under which it created or received the protected health information;

(vi) Section 164.532 relating to transition requirements; and

(vii) Section 164.534 relating to compliance dates for initial implementation of the privacy standards.

(2) When a health care clearinghouse creates or receives protected health information other than as a business associate of a covered entity, the clearinghouse must comply with all of the standards, requirements, and implementation specifications of this subpart.

(c) The standards, requirements, and implementation specifications of this subpart do not apply to the Department of Defense or to any other federal agency, or non-governmental organization acting on its behalf, when providing health care to overseas foreign national beneficiaries.

§ 164.501 Definitions.

As used in this subpart, the following terms have the following meanings:

Correctional institution means any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. *Other persons* held in lawful custody includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial.

Covered functions means those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

Data aggregation means, with respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate with the protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

Designated record set means:

(1) A group of records maintained by or for a covered entity that is:

(i) The medical records and billing records about individuals maintained by or for a covered health care provider;

(ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

(iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.

(2) For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

Direct treatment relationship means a treatment relationship between an individual and a health care provider that is not an indirect treatment relationship.

Disclosure means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

Health care operations means any of the following activities of the covered entity to the extent that the activities are related to covered functions, and any of the following activities of an organized health care arrangement in which the covered entity participates:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

(2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

(3) Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable;

(4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

(5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

(6) Business management and general administrative activities of the entity, including, but not limited to:

(i) Management activities relating to implementation of and compliance with the requirements of this subchapter;

(ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.

(iii) Resolution of internal grievances;

(iv) Due diligence in connection with the sale or transfer of assets to a potential successor in interest, if the potential successor in interest is a covered entity or, following completion of the sale or transfer, will become a covered entity; and

(v) Consistent with the applicable requirements of § 164.514, creating de-identified health information, fundraising for the benefit of the covered entity, and marketing for which an individual authorization is not required as described in § 164.514(e)(2).

Health oversight agency means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

Indirect treatment relationship means a relationship between an individual and a health care provider in which:

(1) The health care provider delivers health care to the individual based on the orders of another health care provider; and

(2) The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual.

Individual means the person who is the subject of protected health information.

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

(i) That identifies the individual; or

(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Inmate means a person incarcerated in or otherwise confined to a correctional institution.

Law enforcement official means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

(1) Investigate or conduct an official inquiry into a potential violation of law; or

(2) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Marketing means to make a communication about a product or service a purpose of which is to encourage recipients of the communication to purchase or use the product or service.

(1) *Marketing* does not include communications that meet the requirements of paragraph (2) of this definition and that are made by a covered entity:

(i) For the purpose of describing the entities participating in a health care provider network or health plan network, or for the purpose of describing if and the extent to which a product or service (or payment for such product or service) is provided by a covered entity or included in a plan of benefits; or

(ii) That are tailored to the circumstances of a particular individual and the communications are:

(A) Made by a health care provider to an individual as part of the treatment of the individual, and for the purpose of furthering the treatment of that individual; or

(B) Made by a health care provider or health plan to an individual in the course of managing the treatment of that individual, or for the purpose of directing or recommending to that individual alternative treatments, therapies, health care providers, or settings of care.

(2) A communication described in paragraph (1) of this definition is not included in marketing if:

(i) The communication is made orally; or

(ii) The communication is in writing and the covered entity does not receive direct or indirect remuneration from a third party for making the communication.

Organized health care arrangement means:

(1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;

(2) An organized system of health care in which more than one covered entity participates, and in which the participating covered entities:

(i) Hold themselves out to the public as participating in a joint arrangement; and

(ii) Participate in joint activities that include at least one of the following:

(A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;

(B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or

(C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

(3) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;

(4) A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or

(5) The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.

Payment means:

(1) The activities undertaken by:

(i) A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or

(ii) A covered health care provider or health plan to obtain or provide reimbursement for the provision of health care; and

(2) The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to:

(i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

(ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics;

(iii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;

(iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

(v) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and

(vi) Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:

(A) Name and address;

(B) Date of birth;

(C) Social security number;

(D) Payment history;

(E) Account number; and

(F) Name and address of the health care provider and/or health plan.

Plan sponsor is defined as defined at section 3(16)(B) of ERISA, 29 U.S.C. 1002(16)(B).

Protected health information means individually identifiable health information:

(1) Except as provided in paragraph (2) of this definition, that is:

(i) Transmitted by electronic media;

(ii) Maintained in any medium described in the definition of *electronic media* at § 162.103 of this subchapter; or

(iii) Transmitted or maintained in any other form or medium.

(2) *Protected health information* excludes individually identifiable health information in:

(i) Education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. 1232g; and

(ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv).

Psychotherapy notes means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. *Psychotherapy notes* excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Public health authority means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

Required by law means a mandate contained in law that compels a covered entity to make a use or disclosure of protected health information and that is enforceable in a court of law. *Required by law* includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

Research means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Treatment means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

§ 164.502 Uses and disclosures of protected health information: general rules.

(a) *Standard.* A covered entity may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

(1) *Permitted uses and disclosures.* A covered entity is permitted to use or disclose protected health information as follows:

(i) To the individual;

(ii) Pursuant to and in compliance with a consent that complies with § 164.506, to carry out treatment, payment, or health care operations;

(iii) Without consent, if consent is not required under § 164.506(a) and has not been sought under § 164.506(a)(4), to carry out treatment, payment, or health care operations, except with respect to psychotherapy notes;

(iv) Pursuant to and in compliance with a valid authorization under § 164.508;

(v) Pursuant to an agreement under, or as otherwise permitted by, § 164.510; and

(vi) As permitted by and in compliance with this section, § 164.512, or § 164.514(e), (f), and (g).

(2) *Required disclosures.* A covered entity is required to disclose protected health information:

(i) To an individual, when requested under, and required by § 164.524 or § 164.528; and

(ii) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subpart.

(b) *Standard: Minimum necessary.* (1) *Minimum necessary applies.* When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

(2) *Minimum necessary does not apply.* This requirement does not apply to:

(i) Disclosures to or requests by a health care provider for treatment;

(ii) Uses or disclosures made to the individual, as permitted under paragraph (a)(1)(i) of this section, as required by paragraph (a)(2)(i) of this section, or pursuant to an authorization under § 164.508, except for authorizations requested by the covered entity under § 164.508(d), (e), or (f);

(iii) Disclosures made to the Secretary in accordance with subpart C of part 160 of this subchapter;

(iv) Uses or disclosures that are required by law, as described by § 164.512(a); and

(v) Uses or disclosures that are required for compliance with applicable requirements of this subchapter.

(c) *Standard: Uses and disclosures of protected health information subject to an agreed upon restriction.* A covered entity that has agreed to a restriction pursuant to § 164.522(a)(1) may not use or disclose the protected health information covered by the restriction in violation of such restriction, except as otherwise provided in § 164.522(a).

(d) *Standard: Uses and disclosures of de-identified protected health information.*

(1) *Uses and disclosures to create de-identified information.* A covered entity may use protected health information to create information that is not individually identifiable health information or disclose protected health information only to a business associate for such purpose, whether or not the de-identified information is to be used by the covered entity.

(2) *Uses and disclosures of de-identified information.* Health information that meets the standard and implementation specifications for de-identification under § 164.514(a) and (b) is considered not to be individually identifiable health information, *i.e.,* de-identified. The requirements of this subpart do not apply to information that has been de-identified in accordance with the applicable requirements of § 164.514, provided that:

(i) Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of protected health information; and

(ii) If de-identified information is re-identified, a covered entity may use or disclose such re-identified information only as permitted or required by this subpart.

(e)(1) *Standard: Disclosures to business associates.* (i) A covered entity may disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information.

(ii) This standard does not apply:

(A) With respect to disclosures by a covered entity to a health care provider concerning the treatment of the individual;

(B) With respect to disclosures by a group health plan or a health insurance issuer or HMO with respect to a group health plan to the plan sponsor, to the extent that the requirements of § 164.504(f) apply and are met; or

(C) With respect to uses or disclosures by a health plan that is a government program providing public benefits, if eligibility for, or enrollment in, the health plan is determined by an agency other than the agency administering the health plan, or if the protected health information used to determine enrollment or eligibility in the health plan is collected by an agency other than the agency administering the health plan, and such activity is authorized by law, with respect to the collection and sharing of individually identifiable health information for the performance of such functions by the health plan and the agency other than the agency administering the health plan.

(iii) A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and § 164.504(e).

(2) *Implementation specification: documentation.* A covered entity must document the satisfactory assurances required by paragraph (e)(1) of this section through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of § 164.504(e).

(f) *Standard: Deceased individuals.* A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual.

(g)(1) *Standard: Personal representatives.* As specified in this paragraph, a covered entity must, except as provided in paragraphs (g)(3) and (g)(5) of this section, treat a personal representative as the individual for purposes of this subchapter.

(2) *Implementation specification: adults and emancipated minors.* If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

(3) *Implementation specification: unemancipated minors.* If under applicable law a parent, guardian, or other person acting *in loco parentis* has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to protected health information pertaining to a health care service, if:

(i) The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative;

(ii) The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting *in loco parentis,* and the minor, a court, or another person authorized by law consents to such health care service; or

(iii) A parent, guardian, or other person acting *in loco parentis* assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.

(4) *Implementation specification: Deceased individuals.* If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

(5) *Implementation specification: Abuse, neglect, endangerment situations.* Notwithstanding a State law or any requirement of this paragraph to the contrary, a covered entity may elect not to treat a person as the personal representative of an individual if:

(i) The covered entity has a reasonable belief that:

(A) The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or

(B) Treating such person as the personal representative could endanger the individual; and

(ii) The covered entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

(h) *Standard: Confidential communications.* A covered health care provider or health plan must comply with the applicable requirements of § 164.522(b) in communicating protected health information.

(i) *Standard: Uses and disclosures consistent with notice.* A covered entity that is required by § 164.520 to have a notice may not use or disclose protected health information in a manner inconsistent with such notice. A covered entity that is required by § 164.520(b)(1)(iii) to include a specific statement in its notice if it intends to engage in an activity listed in § 164.520(b)(1)(iii)(A)–(C), may not use or disclose protected health information for such activities, unless the required statement is included in the notice.

(j) *Standard: Disclosures by whistleblowers and workforce member crime victims.*

(1) *Disclosures by whistleblowers.* A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce or a business associate discloses protected health information, provided that:

(i) The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and

(ii) The disclosure is to:

(A) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or

(B) An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in paragraph (j)(1)(i) of this section.

(2) *Disclosures by workforce members who are victims of a crime.* A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce who is the victim of a criminal act discloses protected health information to a law enforcement official, provided that:

(i) The protected health information disclosed is about the suspected perpetrator of the criminal act; and

(ii) The protected health information disclosed is limited to the information listed in § 164.512(f)(2)(i).

§ 164.504 Uses and disclosures: Organizational requirements.

(a) *Definitions.* As used in this section:

Common control exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity.

Common ownership exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity.

Health care component has the following meaning:

(1) Components of a covered entity that perform covered functions are part of the health care component.

(2) Another component of the covered entity is part of the entity's health care component to the extent that:

(i) It performs, with respect to a component that performs covered functions, activities that would make such other component a business associate of the component that performs covered functions if the two components were separate legal entities; and

(ii) The activities involve the use or disclosure of protected health information that such other component creates or receives from or on behalf of the component that performs covered functions.

Hybrid entity means a single legal entity that is a covered entity and whose covered functions are not its primary functions.

Plan administration functions means administration functions performed by the plan sponsor of a group health plan on behalf of the group health plan and excludes functions performed by the plan sponsor in connection with any other benefit or benefit plan of the plan sponsor.

Summary health information means information, that may be individually identifiable health information, and:

(1) That summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan; and

(2) From which the information described at § 164.514(b)(2)(i) has been deleted, except that the geographic information described in § 164.514(b)(2)(i)(B) need only be aggregated to the level of a five digit zip code.

(b) *Standard: Health care component.* If a covered entity is a hybrid entity, the requirements of this subpart, other than the requirements of this section, apply only to the health care component(s) of the entity, as specified in this section.

(c)(1) *Implementation specification: Application of other provisions.* In applying a provision of this subpart, other than this section, to a hybrid entity:

(i) A reference in such provision to a ''covered entity'' refers to a health care component of the covered entity;

(ii) A reference in such provision to a ''health plan,'' ''covered health care provider,'' or ''health care clearinghouse'' refers to a health care component of the covered entity if such health care component performs the functions of a health plan, covered health care provider, or health care clearinghouse, as applicable; and

(iii) A reference in such provision to ''protected health information'' refers to protected health information that is created or received by or on behalf of the health care component of the covered entity.

(2) *Implementation specifications: Safeguard requirements.* The covered entity that is a hybrid entity must ensure that a health care component of the entity complies with the applicable requirements of this subpart. In particular, and without limiting this requirement, such covered entity must ensure that:

(i) Its health care component does not disclose protected health information to another component of the covered entity in circumstances in which this subpart would prohibit such disclosure if the health care component and the other component were separate and distinct legal entities;

(ii) A component that is described by paragraph (2)(i) of the definition of *health care component* in this section does not use or disclose protected health information that is within paragraph (2)(ii) of such definition for purposes of its activities other than those described by paragraph (2)(i) of such definition in a way prohibited by this subpart; and

(iii) If a person performs duties for both the health care component in the capacity of a member of the workforce of such component and for another component of the entity in the same capacity with respect to that component, such workforce member must not use or disclose protected health information created or received in the course of or incident to the member's work for the health care component in a way prohibited by this subpart.

(3) *Implementation specifications: Responsibilities of the covered entity.* A covered entity that is a hybrid entity has the following responsibilities:

(i) For purposes of subpart C of part 160 of this subchapter, pertaining to compliance and enforcement, the covered entity has the responsibility to comply with this subpart.

(ii) The covered entity has the responsibility for complying with

§ 164.530(i), pertaining to the implementation of policies and procedures to ensure compliance with this subpart, including the safeguard requirements in paragraph (c)(2) of this section.

(iii) The covered entity is responsible for designating the components that are part of one or more health care components of the covered entity and documenting the designation as required by § 164.530(j).

(d)(1) *Standard: Affiliated covered entities.* Legally separate covered entities that are affiliated may designate themselves as a single covered entity for purposes of this subpart.

(2) *Implementation specifications: Requirements for designation of an affiliated covered entity.* (i) Legally separate covered entities may designate themselves (including any health care component of such covered entity) as a single affiliated covered entity, for purposes of this subpart, if all of the covered entities designated are under common ownership or control.

(ii) The designation of an affiliated covered entity must be documented and the documentation maintained as required by § 164.530(j).

(3) *Implementation specifications: Safeguard requirements.* An affiliated covered entity must ensure that:

(i) The affiliated covered entity's use and disclosure of protected health information comply with the applicable requirements of this subpart; and

(ii) If the affiliated covered entity combines the functions of a health plan, health care provider, or health care clearinghouse, the affiliated covered entity complies with paragraph (g) of this section.

(e)(1) *Standard: Business associate contracts.* (i) The contract or other arrangement between the covered entity and the business associate required by § 164.502(e)(2) must meet the requirements of paragraph (e)(2) or (e)(3) of this section, as applicable.

(ii) A covered entity is not in compliance with the standards in § 164.502(e) and paragraph (e) of this section, if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:

(A) Terminated the contract or arrangement, if feasible; or

(B) If termination is not feasible, reported the problem to the Secretary.

(2) *Implementation specifications: Business associate contracts.* A contract between the covered entity and a business associate must:

(i) Establish the permitted and required uses and disclosures of such information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity, except that:

(A) The contract may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate, as provided in paragraph (e)(4) of this section; and

(B) The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.

(ii) Provide that the business associate will:

(A) Not use or further disclose the information other than as permitted or required by the contract or as required by law;

(B) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract;

(C) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware;

(D) Ensure that any agents, including a subcontractor, to whom it provides protected health information received from, or created or received by the business associate on behalf of, the covered entity agrees to the same restrictions and conditions that apply to the business associate with respect to such information;

(E) Make available protected health information in accordance with § 164.524;

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with § 164.526;

(G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528;

(H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and

(I) At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

(iii) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

(3) *Implementation specifications: Other arrangements.* (i) If a covered entity and its business associate are both governmental entities:

(A) The covered entity may comply with paragraph (e) of this section by entering into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (e)(2) of this section.

(B) The covered entity may comply with paragraph (e) of this section, if other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (e)(2) of this section.

(ii) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of *business associate* in § 160.103 of this subchapter to a covered entity, such covered entity may disclose protected health information to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements of this paragraph (e), provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (e)(3)(i) of this section, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained.

(iii) The covered entity may omit from its other arrangements the termination authorization required by paragraph (e)(2)(iii) of this section, if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.

(4) *Implementation specifications: Other requirements for contracts and other arrangements.* (i) The contract or other arrangement between the covered entity and the business associate may

permit the business associate to use the information received by the business associate in its capacity as a business associate to the covered entity, if necessary:

(A) For the proper management and administration of the business associate; or

(B) To carry out the legal responsibilities of the business associate.

(ii) The contract or other arrangement between the covered entity and the business associate may permit the business associate to disclose the information received by the business associate in its capacity as a business associate for the purposes described in paragraph (e)(4)(i) of this section, if:

(A) The disclosure is required by law; or

(B)(*1*) The business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person; and

(*2*) The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(f)(1) *Standard: Requirements for group health plans.* (i) Except as provided under paragraph (f)(1)(ii) of this section or as otherwise authorized under § 164.508, a group health plan, in order to disclose protected health information to the plan sponsor or to provide for or permit the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO with respect to the group health plan, must ensure that the plan documents restrict uses and discloses of such information by the plan sponsor consistent with the requirements of this subpart.

(ii) The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose summary health information to the plan sponsor, if the plan sponsor requests the summary health information for the purpose of :

(A) Obtaining premium bids from health plans for providing health insurance coverage under the group health plan; or

(B) Modifying, amending, or terminating the group health plan.

(2) *Implementation specifications: Requirements for plan documents.* The plan documents of the group health plan must be amended to incorporate provisions to:

(i) Establish the permitted and required uses and disclosures of such information by the plan sponsor, provided that such permitted and required uses and disclosures may not be inconsistent with this subpart.

(ii) Provide that the group health plan will disclose protected health information to the plan sponsor only upon receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate the following provisions and that the plan sponsor agrees to:

(A) Not use or further disclose the information other than as permitted or required by the plan documents or as required by law;

(B) Ensure that any agents, including a subcontractor, to whom it provides protected health information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;

(C) Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor;

(D) Report to the group health plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware;

(E) Make available protected health information in accordance with § 164.524;

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with § 164.526;

(G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528;

(H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from the group health plan available to the Secretary for purposes of determining compliance by the group health plan with this subpart;

(I) If feasible, return or destroy all protected health information received from the group health plan that the sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and

(J) Ensure that the adequate separation required in paragraph (f)(2)(iii) of this section is established.

(iii) Provide for adequate separation between the group health plan and the plan sponsor. The plan documents must:

(A) Describe those employees or classes of employees or other persons under the control of the plan sponsor to be given access to the protected health information to be disclosed, provided that any employee or person who receives protected health information relating to payment under, health care operations of, or other matters pertaining to the group health plan in the ordinary course of business must be included in such description;

(B) Restrict the access to and use by such employees and other persons described in paragraph (f)(2)(iii)(A) of this section to the plan administration functions that the plan sponsor performs for the group health plan; and

(C) Provide an effective mechanism for resolving any issues of noncompliance by persons described in paragraph (f)(2)(iii)(A) of this section with the plan document provisions required by this paragraph.

(3) *Implementation specifications: Uses and disclosures.* A group health plan may:

(i) Disclose protected health information to a plan sponsor to carry out plan administration functions that the plan sponsor performs only consistent with the provisions of paragraph (f)(2) of this section;

(ii) Not permit a health insurance issuer or HMO with respect to the group health plan to disclose protected health information to the plan sponsor except as permitted by this paragraph;

(iii) Not disclose and may not permit a health insurance issuer or HMO to disclose protected health information to a plan sponsor as otherwise permitted by this paragraph unless a statement required by § 164.520(b)(1)(iii)(C) is included in the appropriate notice; and (iv) Not disclose protected health information to the plan sponsor for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the plan sponsor.

(g) *Standard: Requirements for a covered entity with multiple covered functions.*

(1) A covered entity that performs multiple covered functions that would make the entity any combination of a health plan, a covered health care provider, and a health care clearinghouse, must comply with the standards, requirements, and implementation specifications of this subpart, as applicable to the health plan, health care provider, or health care clearinghouse covered functions performed.

(2) A covered entity that performs multiple covered functions may use or disclose the protected health information of individuals who receive the covered entity's health plan or health care provider services, but not both, only for purposes related to the appropriate function being performed.

§ 164.506 Consent for uses or disclosures to carry out treatment, payment, or health care operations.

(a) *Standard: Consent requirement.* (1) Except as provided in paragraph (a)(2) or (a)(3) of this section, a covered health care provider must obtain the individual's consent, in accordance with this section, prior to using or disclosing protected health information to carry out treatment, payment, or health care operations.

(2) A covered health care provider may, without consent, use or disclose protected health information to carry out treatment, payment, or health care operations, if:

(i) The covered health care provider has an indirect treatment relationship with the individual; or

(ii) The covered health care provider created or received the protected health information in the course of providing health care to an individual who is an inmate.

(3)(i) A covered health care provider may, without prior consent, use or disclose protected health information created or received under paragraph (a)(3)(i)(A)–(C) of this section to carry out treatment, payment, or health care operations:

(A) In emergency treatment situations, if the covered health care provider attempts to obtain such consent as soon as reasonably practicable after the delivery of such treatment;

(B) If the covered health care provider is required by law to treat the individual, and the covered health care provider attempts to obtain such consent but is unable to obtain such consent; or

(C) If a covered health care provider attempts to obtain such consent from the individual but is unable to obtain such consent due to substantial barriers to communicating with the individual, and the covered health care provider determines, in the exercise of professional judgment, that the individual's consent to receive treatment is clearly inferred from the circumstances.

(ii) A covered health care provider that fails to obtain such consent in accordance with paragraph (a)(3)(i) of this section must document its attempt to obtain consent and the reason why consent was not obtained.

(4) If a covered entity is not required to obtain consent by paragraph (a)(1) of this section, it may obtain an individual's consent for the covered entity's own use or disclosure of protected health information to carry out treatment, payment, or health care operations, provided that such consent meets the requirements of this section.

(5) Except as provided in paragraph (f)(1) of this section, a consent obtained by a covered entity under this section is not effective to permit another covered entity to use or disclose protected health information.

(b) *Implementation specifications: General requirements.* (1) A covered health care provider may condition treatment on the provision by the individual of a consent under this section.

(2) A health plan may condition enrollment in the health plan on the provision by the individual of a consent under this section sought in conjunction with such enrollment.

(3) A consent under this section may not be combined in a single document with the notice required by § 164.520.

(4)(i) A consent for use or disclosure may be combined with other types of written legal permission from the individual (*e.g.,* an informed consent for treatment or a consent to assignment of benefits), if the consent under this section:

(A) Is visually and organizationally separate from such other written legal permission; and

(B) Is separately signed by the individual and dated.

(ii) A consent for use or disclosure may be combined with a research authorization under § 164.508(f).

(5) An individual may revoke a consent under this section at any time, except to the extent that the covered entity has taken action in reliance thereon. Such revocation must be in writing.

(6) A covered entity must document and retain any signed consent under this section as required by § 164.530(j).

(c) *Implementation specifications: Content requirements.* A consent under this section must be in plain language and:

(1) Inform the individual that protected health information may be used and disclosed to carry out treatment, payment, or health care operations;

(2) Refer the individual to the notice required by § 164.520 for a more complete description of such uses and disclosures and state that the individual has the right to review the notice prior to signing the consent;

(3) If the covered entity has reserved the right to change its privacy practices that are described in the notice in accordance with § 164.520(b)(1)(v)(C), state that the terms of its notice may change and describe how the individual may obtain a revised notice;

(4) State that:

(i) The individual has the right to request that the covered entity restrict how protected health information is used or disclosed to carry out treatment, payment, or health care operations;

(ii) The covered entity is not required to agree to requested restrictions; and

(iii) If the covered entity agrees to a requested restriction, the restriction is binding on the covered entity;

(5) State that the individual has the right to revoke the consent in writing, except to the extent that the covered entity has taken action in reliance thereon; and

(6) Be signed by the individual and dated.

(d) *Implementation specifications: Defective consents.* There is no consent under this section, if the document submitted has any of the following defects:

(1) The consent lacks an element required by paragraph (c) of this section, as applicable; or

(2) The consent has been revoked in accordance with paragraph (b)(5) of this section.

(e) *Standard: Resolving conflicting consents and authorizations.* (1) If a covered entity has obtained a consent under this section and receives any other authorization or written legal permission from the individual for a disclosure of protected health information to carry out treatment, payment, or health care operations, the covered entity may disclose such protected health information only in accordance with the more restrictive consent, authorization, or other written legal permission from the individual.

(2) A covered entity may attempt to resolve a conflict between a consent and an authorization or other written legal permission from the individual described in paragraph (e)(1) of this section by:

(i) Obtaining a new consent from the individual under this section for the disclosure to carry out treatment, payment, or health care operations; or

(ii) Communicating orally or in writing with the individual in order to determine the individual's preference in resolving the conflict. The covered entity must document the individual's preference and may only disclose protected health information in accordance with the individual's preference.

(f)(1) *Standard: Joint consents.* Covered entities that participate in an organized health care arrangement and that have a joint notice under § 164.520(d) may comply with this section by a joint consent.

(2) *Implementation specifications: Requirements for joint consents.* (i) A joint consent must:

(A) Include the name or other specific identification of the covered entities, or classes of covered entities, to which the joint consent applies; and

(B) Meet the requirements of this section, except that the statements required by this section may be altered to reflect the fact that the consent covers more than one covered entity.

(ii) If an individual revokes a joint consent, the covered entity that receives the revocation must inform the other entities covered by the joint consent of the revocation as soon as practicable.

§ 164.508 Uses and disclosures for which an authorization is required.

(a) *Standard: Authorizations for uses and disclosures.* (1) *Authorization required: General rule.* Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization.

(2) *Authorization required: psychotherapy notes.* Notwithstanding any other provision of this subpart, other than transition provisions provided for in § 164.532, a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:

(i) To carry out the following treatment, payment, or health care operations, consistent with consent requirements in § 164.506:

(A) Use by originator of the psychotherapy notes for treatment;

(B) Use or disclosure by the covered entity in training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or

(C) Use or disclosure by the covered entity to defend a legal action or other proceeding brought by the individual; and

(ii) A use or disclosure that is required by § 164.502(a)(2)(ii) or permitted by § 164.512(a); § 164.512(d) with respect to the oversight of the originator of the psychotherapy notes; § 164.512(g)(1); or § 164.512(j)(1)(i).

(b) *Implementation specifications: General requirements.*—(1) *Valid authorizations.*

(i) A valid authorization is a document that contains the elements listed in paragraph (c) and, as applicable, paragraph (d), (e), or (f) of this section.

(ii) A valid authorization may contain elements or information in addition to the elements required by this section, provided that such additional elements or information are not be inconsistent with the elements required by this section.

(2) *Defective authorizations.* An authorization is not valid, if the document submitted has any of the following defects:

(i) The expiration date has passed or the expiration event is known by the covered entity to have occurred;

(ii) The authorization has not been filled out completely, with respect to an element described by paragraph (c), (d), (e), or (f) of this section, if applicable;

(iii) The authorization is known by the covered entity to have been revoked;

(iv) The authorization lacks an element required by paragraph (c), (d), (e), or (f) of this section, if applicable;

(v) The authorization violates paragraph (b)(3) of this section, if applicable;

(vi) Any material information in the authorization is known by the covered entity to be false.

(3) *Compound authorizations.* An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization, except as follows:

(i) An authorization for the use or disclosure of protected health information created for research that includes treatment of the individual may be combined as permitted by § 164.506(b)(4)(ii) or paragraph (f) of this section;

(ii) An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes;

(iii) An authorization under this section, other than an authorization for a use or disclosure of psychotherapy notes may be combined with any other such authorization under this section, except when a covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits under paragraph (b)(4) of this section on the provision of one of the authorizations.

(4) *Prohibition on conditioning of authorizations.* A covered entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except:

(i) A covered health care provider may condition the provision of research-related treatment on provision of an authorization under paragraph (f) of this section;

(ii) A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan prior to an individual's enrollment in the health plan, if:

(A) The authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations; and

(B) The authorization is not for a use or disclosure of psychotherapy notes under paragraph (a)(2) of this section;

(iii) A health plan may condition payment of a claim for specified benefits on provision of an authorization under paragraph (e) of this section, if:

(A) The disclosure is necessary to determine payment of such claim; and

(B) The authorization is not for a use or disclosure of psychotherapy notes under paragraph (a)(2) of this section; and

(iv) A covered entity may condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party on provision of an authorization for the disclosure of the protected health information to such third party.

(5) *Revocation of authorizations.* An individual may revoke an authorization provided under this section at any time, provided that the revocation is in writing, except to the extent that:

(i) The covered entity has taken action in reliance thereon; or

(ii) If the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy.

(6) *Documentation.* A covered entity must document and retain any signed authorization under this section as required by § 164.530(j).

(c) *Implementation specifications: Core elements and requirements.* (1) *Core elements.* A valid authorization under this section must contain at least the following elements:

(i) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;

(ii) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;

(iii) The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure;

(iv) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure;

(v) A statement of the individual's right to revoke the authorization in writing and the exceptions to the right to revoke, together with a description of how the individual may revoke the authorization;

(vi) A statement that information used or disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer be protected by this rule;

(vii) Signature of the individual and date; and

(viii) If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual.

(2) *Plain language requirement.* The authorization must be written in plain language.

(d) *Implementation specifications: Authorizations requested by a covered entity for its own uses and disclosures.* If an authorization is requested by a covered entity for its own use or disclosure of protected health information that it maintains, the covered entity must comply with the following requirements.

(1) *Required elements.* The authorization for the uses or disclosures described in this paragraph must, in addition to meeting the requirements of paragraph (c) of this section, contain the following elements:

(i) For any authorization to which the prohibition on conditioning in paragraph (b)(4) of this section applies, a statement that the covered entity will not condition treatment, payment, enrollment in the health plan, or eligibility for benefits on the individual's providing authorization for the requested use or disclosure;

(ii) A description of each purpose of the requested use or disclosure;

(iii) A statement that the individual may:

(A) Inspect or copy the protected health information to be used or disclosed as provided in § 164.524; and

(B) Refuse to sign the authorization; and

(iv) If use or disclosure of the requested information will result in direct or indirect remuneration to the covered entity from a third party, a statement that such remuneration will result.

(2) *Copy to the individual.* A covered entity must provide the individual with a copy of the signed authorization.

(e) *Implementation specifications: Authorizations requested by a covered entity for disclosures by others.* If an authorization is requested by a covered entity for another covered entity to disclose protected health information to the covered entity requesting the authorization to carry out treatment, payment, or health care operations, the covered entity requesting the authorization must comply with the following requirements.

(1) *Required elements.* The authorization for the disclosures described in this paragraph must, in addition to meeting the requirements of paragraph (c) of this section, contain the following elements:

(i) A description of each purpose of the requested disclosure;

(ii) Except for an authorization on which payment may be conditioned under paragraph (b)(4)(iii) of this section, a statement that the covered entity will not condition treatment, payment, enrollment in the health plan, or eligibility for benefits on the individual's providing authorization for the requested use or disclosure; and

(iii) A statement that the individual may refuse to sign the authorization.

(2) *Copy to the individual.* A covered entity must provide the individual with a copy of the signed authorization.

(f) *Implementation specifications: Authorizations for uses and disclosures of protected health information created for research that includes treatment of the individual.*

(1) *Required elements.* Except as otherwise permitted by § 164.512(i), a covered entity that creates protected health information for the purpose, in whole or in part, of research that includes treatment of individuals must obtain an authorization for the use or disclosure of such information. Such authorization must:

(i) For uses and disclosures not otherwise permitted or required under this subpart, meet the requirements of paragraphs (c) and (d) of this section; and

(ii) Contain:

(A) A description of the extent to which such protected health information will be used or disclosed to carry out treatment, payment, or health care operations;

(B) A description of any protected health information that will not be used or disclosed for purposes permitted in accordance with §§ 164.510 and 164.512, provided that the covered entity may not include a limitation affecting its right to make a use or disclosure that is required by law or permitted by § 164.512(j)(1)(i); and

(C) If the covered entity has obtained or intends to obtain the individual's consent under § 164.506, or has provided or intends to provide the individual with a notice under § 164.520, the authorization must refer to that consent or notice, as applicable, and state that the statements made pursuant to this section are binding.

(2) *Optional procedure.* An authorization under this paragraph may be in the same document as:

(i) A consent to participate in the research;

(ii) A consent to use or disclose protected health information to carry out treatment, payment, or health care operations under § 164.506; or

(iii) A notice of privacy practices under § 164.520.

§ 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.

A covered entity may use or disclose protected health information without the written consent or authorization of the individual as described by §§ 164.506 and 164.508, respectively, provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the disclosure in accordance with the applicable requirements of this section. The covered entity may orally inform the individual of and obtain the individual's oral agreement or objection to a use or disclosure permitted by this section.

(a) *Standard: use and disclosure for facility directories.* (1) *Permitted uses and disclosure.* Except when an objection is expressed in accordance with paragraphs (a)(2) or (3) of this section, a covered health care provider may:

(i) Use the following protected health information to maintain a directory of individuals in its facility:

(A) The individual's name;

(B) The individual's location in the covered health care provider's facility;

(C) The individual's condition described in general terms that does not communicate specific medical information about the individual; and

(D) The individual's religious affiliation; and

(ii) Disclose for directory purposes such information:

(A) To members of the clergy; or

(B) Except for religious affiliation, to other persons who ask for the individual by name.

(2) *Opportunity to object.* A covered health care provider must inform an individual of the protected health information that it may include in a directory and the persons to whom it may disclose such information (including disclosures to clergy of information regarding religious affiliation) and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures permitted by paragraph (a)(1) of this section.

(3) *Emergency circumstances.* (i) If the opportunity to object to uses or disclosures required by paragraph (a)(2) of this section cannot practicably be provided because of the individual's incapacity or an emergency treatment circumstance, a covered health care provider may use or disclose some or all of the protected health information permitted by paragraph (a)(1) of this section for the facility's directory, if such disclosure is:

(A) Consistent with a prior expressed preference of the individual, if any, that is known to the covered health care provider; and

(B) In the individual's best interest as determined by the covered health care provider, in the exercise of professional judgment.

(ii) The covered health care provider must inform the individual and provide an opportunity to object to uses or disclosures for directory purposes as required by paragraph (a)(2) of this section when it becomes practicable to do so.

(b) *Standard: uses and disclosures for involvement in the individual's care and notification purposes.* (1) *Permitted uses and disclosures.* (i) A covered entity may, in accordance with paragraphs (b)(2) or (3) of this section, disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the protected health information directly relevant to such person's involvement with the individual's care or payment related to the individual's health care.

(ii) A covered entity may use or disclose protected health information to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. Any such use or disclosure of protected health information for such notification purposes must be in accordance with paragraphs (b)(2), (3), or (4) of this section, as applicable.

(2) *Uses and disclosures with the individual present.* If the individual is present for, or otherwise available prior to, a use or disclosure permitted by paragraph (b)(1) of this section and has the capacity to make health care decisions, the covered entity may use or disclose the protected health information if it:

(i) Obtains the individual's agreement;

(ii) Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or

(iii) Reasonably infers from the circumstances, based the exercise of professional judgment, that the individual does not object to the disclosure.

(3) *Limited uses and disclosures when the individual is not present.* If the individual is not present for, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's health care. A covered entity may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information.

(4) *Use and disclosures for disaster relief purposes.* A covered entity may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b)(1)(ii) of this section. The requirements in paragraphs (b)(2) and (3) of this section apply to such uses and disclosure to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

§ 164.512 Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required.

A covered entity may use or disclose protected health information without the written consent or authorization of the individual as described in §§ 164.506 and 164.508, respectively, or the opportunity for the individual to agree or object as described in § 164.510, in the situations covered by this section, subject to the applicable requirements of this section. When the covered entity is required by this section to inform the individual of, or when the individual may agree to, a use or disclosure permitted by this section, the covered entity's information and the individual's agreement may be given orally.

(a) *Standard: Uses and disclosures required by law.* (1) A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.

(2) A covered entity must meet the requirements described in paragraph (c), (e), or (f) of this section for uses or disclosures required by law.

(b) *Standard: uses and disclosures for public health activities.* (1) *Permitted disclosures.* A covered entity may disclose protected health information for the public health activities and purposes described in this paragraph to:

(i) A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;

(ii) A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;

(iii) A person subject to the jurisdiction of the Food and Drug Administration:

(A) To report adverse events (or similar reports with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations if the disclosure is made to the person required or directed to report such information to the Food and Drug Administration;

(B) To track products if the disclosure is made to a person required or directed by the Food and Drug Administration to track the product;

(C) To enable product recalls, repairs, or replacement (including locating and

notifying individuals who have received products of product recalls, withdrawals, or other problems); or

(D) To conduct post marketing surveillance to comply with requirements or at the direction of the Food and Drug Administration;

(iv) A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation; or

(v) An employer, about an individual who is a member of the workforce of the employer, if:

(A) The covered entity is a covered health care provider who is a member of the workforce of such employer or who provides a health care to the individual at the request of the employer:

(1) To conduct an evaluation relating to medical surveillance of the workplace; or

(2) To evaluate whether the individual has a work-related illness or injury;

(B) The protected health information that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;

(C) The employer needs such findings in order to comply with its obligations, under 29 CFR parts 1904 through 1928, 30 CFR parts 50 through 90, or under state law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance;

(D) The covered health care provider provides written notice to the individual that protected health information relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer:

(1) By giving a copy of the notice to the individual at the time the health care is provided; or

(2) If the health care is provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care is provided.

(2) *Permitted uses.* If the covered entity also is a public health authority, the covered entity is permitted to use protected health information in all cases in which it is permitted to disclose such information for public health activities under paragraph (b)(1) of this section.

(c) *Standard: Disclosures about victims of abuse, neglect or domestic violence.* (1) *Permitted disclosures.* Except for reports of child abuse or neglect permitted by paragraph (b)(1)(ii) of this section, a covered entity may disclose protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence:

(i) To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law;

(ii) If the individual agrees to the disclosure; or

(iii) To the extent the disclosure is expressly authorized by statute or regulation and:

(A) The covered entity, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or

(B) If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the protected health information for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

(2) *Informing the individual.* A covered entity that makes a disclosure permitted by paragraph (c)(1) of this section must promptly inform the individual that such a report has been or will be made, except if:

(i) The covered entity, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or

(ii) The covered entity would be informing a personal representative, and the covered entity reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

(d) *Standard: Uses and disclosures for health oversight activities.* (1) *Permitted disclosures.* A covered entity may disclose protected health information to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of:

(i) The health care system;

(ii) Government benefit programs for which health information is relevant to beneficiary eligibility;

(iii) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or

(iv) Entities subject to civil rights laws for which health information is necessary for determining compliance.

(2) *Exception to health oversight activities.* For the purpose of the disclosures permitted by paragraph (d)(1) of this section, a health oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:

(i) The receipt of health care;

(ii) A claim for public benefits related to health; or

(iii) Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.

(3) *Joint activities or investigations.* Nothwithstanding paragraph (d)(2) of this section, if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity for purposes of paragraph (d) of this section.

(4) *Permitted uses.* If a covered entity also is a health oversight agency, the covered entity may use protected health information for health oversight activities as permitted by paragraph (d) of this section.

(e) *Standard: Disclosures for judicial and administrative proceedings.*

(1) *Permitted disclosures.* A covered entity may disclose protected health information in the course of any judicial or administrative proceeding:

(i) In response to an order of a court or administrative tribunal, provided that the covered entity discloses only the protected health information expressly authorized by such order; or

(ii) In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if:

(A) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iii) of this section, from the party seeking the information that reasonable efforts have been made by

such party to ensure that the individual who is the subject of the protected health information that has been requested has been given notice of the request; or

(B) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iv) of this section, from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the requirements of paragraph (e)(1)(v) of this section.

(iii) For the purposes of paragraph (e)(1)(ii)(A) of this section, a covered entity receives satisfactory assurances from a party seeking protecting health information if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:

(A) The party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);

(B) The notice included sufficient information about the litigation or proceeding in which the protected health information is requested to permit the individual to raise an objection to the court or administrative tribunal; and

(C) The time for the individual to raise objections to the court or administrative tribunal has elapsed, and:

(*1*) No objections were filed; or

(*2*) All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.

(iv) For the purposes of paragraph (e)(1)(ii)(B) of this section, a covered entity receives satisfactory assurances from a party seeking protected health information, if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:

(A) The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or

(B) The party seeking the protected health information has requested a qualified protective order from such court or administrative tribunal.

(v) For purposes of paragraph (e)(1) of this section, a qualified protective order means, with respect to protected health information requested under paragraph (e)(1)(ii) of this section, an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:

(A) Prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and

(B) Requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding.

(vi) Nothwithstanding paragraph (e)(1)(ii) of this section, a covered entity may disclose protected health information in response to lawful process described in paragraph (e)(1)(ii) of this section without receiving satisfactory assurance under paragraph (e)(1)(ii)(A) or (B) of this section, if the covered entity makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of paragraph (e)(1)(iii) of this section or to seek a qualified protective order sufficient to meet the requirements of paragraph (e)(1)(iv) of this section.

(2) *Other uses and disclosures under this section.* The provisions of this paragraph do not supersede other provisions of this section that otherwise permit or restrict uses or disclosures of protected health information.

(f) *Standard: Disclosures for law enforcement purposes.* A covered entity may disclose protected health information for a law enforcement purpose to a law enforcement official if the conditions in paragraphs (f)(1) through (f)(6) of this section are met, as applicable.

(1) *Permitted disclosures: Pursuant to process and as otherwise required by law.* A covered entity may disclose protected health information:

(i) As required by law including laws that require the reporting of certain types of wounds or other physical injuries, except for laws subject to paragraph (b)(1)(ii) or (c)(1)(i) of this section; or

(ii) In compliance with and as limited by the relevant requirements of:

(A) A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;

(B) A grand jury subpoena; or

(C) An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:

(1) The information sought is relevant and material to a legitimate law enforcement inquiry;

(2) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and

(*3*) De-identified information could not reasonably be used.

(2) *Permitted disclosures: Limited information for identification and location purposes.* Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that:

(i) The covered entity may disclose only the following information:

(A) Name and address;

(B) Date and place of birth;

(C) Social security number;

(D) ABO blood type and rh factor;

(E) Type of injury;

(F) Date and time of treatment;

(G) Date and time of death, if applicable; and

(H) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

(ii) Except as permitted by paragraph (f)(2)(i) of this section, the covered entity may not disclose for the purposes of identification or location under paragraph (f)(2) of this section any protected health information related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

(3) *Permitted disclosure: Victims of a crime.* Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime, other than disclosures that are subject to paragraph (b) or (c) of this section, if:

(ii) The individual agrees to the disclosure; or

(iii) The covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:

(A) The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;

(B) The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and

adversely affected by waiting until the individual is able to agree to the disclosure; and

(C) The disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

(4) *Permitted disclosure: Decedents.* A covered entity may disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the covered entity has a suspicion that such death may have resulted from criminal conduct.

(5) *Permitted disclosure: Crime on premises.* A covered entity may disclose to a law enforcement official protected health information that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity.

(6) *Permitted disclosure: Reporting crime in emergencies.* (i) A covered health care provider providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, may disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to:

(A) The commission and nature of a crime;

(B) The location of such crime or of the victim(s) of such crime; and

(C) The identity, description, and location of the perpetrator of such crime.

(ii) If a covered health care provider believes that the medical emergency described in paragraph (f)(6)(i) of this section is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care, paragraph (f)(6)(i) of this section does not apply and any disclosure to a law enforcement official for law enforcement purposes is subject to paragraph (c) of this section.

(g) *Standard: Uses and disclosures about decedents.* (1) *Coroners and medical examiners.* A covered entity may disclose protected health information to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. A covered entity that also performs the duties of a coroner or medical examiner may use protected health information for the purposes described in this paragraph.

(2) *Funeral directors.* A covered entity may disclose protected health information to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If necessary for funeral directors carry out their duties, the covered entity may disclose the protected health information prior to, and in reasonable anticipation of, the individual's death.

(h) *Standard: Uses and disclosures for cadaveric organ, eye or tissue donation purposes.* A covered entity may use or disclose protected health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.

(i) *Standard: Uses and disclosures for research purposes.* (1) *Permitted uses and disclosures.* A covered entity may use or disclose protected health information for research, regardless of the source of funding of the research, provided that:

(i) *Board approval of a waiver of authorization.* The covered entity obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization required by § 164.508 for use or disclosure of protected health information has been approved by either:

(A) An Institutional Review Board (IRB), established in accordance with 7 CFR lc.107, 10 CFR 745.107, 14 CFR 1230.107, 15 CFR 27.107, 16 CFR 1028.107, 21 CFR 56.107, 22 CFR 225.107, 24 CFR 60.107, 28 CFR 46.107, 32 CFR 219.107, 34 CFR 97.107, 38 CFR 16.107, 40 CFR 26.107, 45 CFR 46.107, 45 CFR 690.107, or 49 CFR 11.107; or

(B) A privacy board that:

(*1*) Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests;

(*2*) Includes at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and

(*3*) Does not have any member participating in a review of any project in which the member has a conflict of interest.

(ii) *Reviews preparatory to research.* The covered entity obtains from the researcher representations that:

(A) Use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research;

(B) No protected health information is to be removed from the covered entity by the researcher in the course of the review; and

(C) The protected health information for which use or access is sought is necessary for the research purposes.

(iii) *Research on decedent's information.* The covered entity obtains from the researcher:

(A) Representation that the use or disclosure is sought is solely for research on the protected health information of decedents;

(B) Documentation, at the request of the covered entity, of the death of such individuals; and

(C) Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.

(2) *Documentation of waiver approval.* For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, under paragraph (i)(1)(i) of this section, the documentation must include all of the following:

(i) *Identification and date of action.* A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved;

(ii) *Waiver criteria.* A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:

(A) The use or disclosure of protected health information involves no more than minimal risk to the individuals;

(B) The alteration or waiver will not adversely affect the privacy rights and the welfare of the individuals;

(C) The research could not practicably be conducted without the alteration or waiver;

(D) The research could not practicably be conducted without access to and use of the protected health information;

(E) The privacy risks to individuals whose protected health information is to be used or disclosed are reasonable in relation to the anticipated benefits if any to the individuals, and the importance of the knowledge that may reasonably be expected to result from the research;

(F) There is an adequate plan to protect the identifiers from improper use and disclosure;

(G) There is an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers, or such retention is otherwise required by law; and

(H) There are adequate written assurances that the protected health

information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of protected health information would be permitted by this subpart.

(iii) *Protected health information needed.* A brief description of the protected health information for which use or access has been determined to be necessary by the IRB or privacy board has determined, pursuant to paragraph (i)(2)(ii)(D) of this section;

(iv) *Review and approval procedures.* A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures, as follows:

(A) An IRB must follow the requirements of the Common Rule, including the normal review procedures (7 CFR 1c.108(b), 10 CFR 745.108(b), 14 CFR 1230.108(b), 15 CFR 27.108(b), 16 CFR 1028.108(b), 21 CFR 56.108(b), 22 CFR 225.108(b), 24 CFR 60.108(b), 28 CFR 46.108(b), 32 CFR 219.108(b), 34 CFR 97.108(b), 38 CFR 16.108(b), 40 CFR 26.108(b), 45 CFR 46.108(b), 45 CFR 690.108(b), or 49 CFR 11.108(b)) or the expedited review procedures (7 CFR 1c.110, 10 CFR 745.110, 14 CFR 1230.110, 15 CFR 27.110, 16 CFR 1028.110, 21 CFR 56.110, 22 CFR 225.110, 24 CFR 60.110, 28 CFR 46.110, 32 CFR 219.110, 34 CFR 97.110, 38 CFR 16.110, 40 CFR 26.110, 45 CFR 46.110, 45 CFR 690.110, or 49 CFR 11.110);

(B) A privacy board must review the proposed research at convened meetings at which a majority of the privacy board members are present, including at least one member who satisfies the criterion stated in paragraph (i)(1)(i)(B)(2) of this section, and the alteration or waiver of authorization must be approved by the majority of the privacy board members present at the meeting, unless the privacy board elects to use an expedited review procedure in accordance with paragraph (i)(2)(iv)(C) of this section;

(C) A privacy board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the protected health information for which use or disclosure is being sought. If the privacy board elects to use an expedited review procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the privacy board, or by one or more members of the privacy board as designated by the chair; and

(v) *Required signature.* The documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair, of the IRB or the privacy board, as applicable.

(j) *Standard: Uses and disclosures to avert a serious threat to health or safety.* (1) *Permitted disclosures.* A covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if the covered entity, in good faith, believes the use or disclosure:

(i)(A) Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and

(B) Is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or

(ii) Is necessary for law enforcement authorities to identify or apprehend an individual:

(A) Because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim; or

(B) Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody, as those terms are defined in § 164.501.

(2) *Use or disclosure not permitted.* A use or disclosure pursuant to paragraph (j)(1)(ii)(A) of this section may not be made if the information described in paragraph (j)(1)(ii)(A) of this section is learned by the covered entity:

(i) In the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure under paragraph (j)(1)(ii)(A) of this section, or counseling or therapy; or

(ii) Through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy described in paragraph (j)(2)(i) of this section.

(3) *Limit on information that may be disclosed.* A disclosure made pursuant to paragraph (j)(1)(ii)(A) of this section shall contain only the statement described in paragraph (j)(1)(ii)(A) of this section and the protected health information described in paragraph (f)(2)(i) of this section.

(4) *Presumption of good faith belief.* A covered entity that uses or discloses protected health information pursuant to paragraph (j)(1) of this section is presumed to have acted in good faith with regard to a belief described in paragraph (j)(1)(i) or (ii) of this section, if the belief is based upon the covered entity's actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.

(k) *Standard: Uses and disclosures for specialized government functions.* (1) *Military and veterans activities.* (i) *Armed Forces personnel.* A covered entity may use and disclose the protected health information of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the appropriate military authority has published by notice in the **Federal Register** the following information:

(A) Appropriate military command authorities; and

(B) The purposes for which the protected health information may be used or disclosed.

(ii) *Separation or discharge from military service.* A covered entity that is a component of the Departments of Defense or Transportation may disclose to the Department of Veterans Affairs (DVA) the protected health information of an individual who is a member of the Armed Forces upon the separation or discharge of the individual from military service for the purpose of a determination by DVA of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs.

(iii) *Veterans.* A covered entity that is a component of the Department of Veterans Affairs may use and disclose protected health information to components of the Department that determine eligibility for or entitlement to, or that provide, benefits under the laws administered by the Secretary of Veterans Affairs.

(iv) *Foreign military personnel.* A covered entity may use and disclose the protected health information of individuals who are foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for Armed Forces personnel under the notice published in the **Federal Register** pursuant to paragraph (k)(1)(i) of this section.

(2) *National security and intelligence activities.* A covered entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, *et seq.*) and implementing authority (*e.g.,* Executive Order 12333).

(3) *Protective services for the President and others.* A covered entity may disclose protected health

information to authorized federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or to for the conduct of investigations authorized by 18 U.S.C. 871 and 879.

(4) *Medical suitability determinations.* A covered entity that is a component of the Department of State may use protected health information to make medical suitability determinations and may disclose whether or not the individual was determined to be medically suitable to the officials in the Department of State who need access to such information for the following purposes:

(i) For the purpose of a required security clearance conducted pursuant to Executive Orders 10450 and 12698;

(ii) As necessary to determine worldwide availability or availability for mandatory service abroad under sections 101(a)(4) and 504 of the Foreign Service Act; or

(iii) For a family to accompany a Foreign Service member abroad, consistent with section 101(b)(5) and 904 of the Foreign Service Act.

(5) *Correctional institutions and other law enforcement custodial situations.* (i) *Permitted disclosures.* A covered entity may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual protected health information about such inmate or individual, if the correctional institution or such law enforcement official represents that such protected health information is necessary for:

(A) The provision of health care to such individuals;

(B) The health and safety of such individual or other inmates;

(C) The health and safety of the officers or employees of or others at the correctional institution;

(D) The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;

(E) Law enforcement on the premises of the correctional institution; and

(F) The administration and maintenance of the safety, security, and good order of the correctional institution.

(ii) *Permitted uses.* A covered entity that is a correctional institution may use protected health information of individuals who are inmates for any purpose for which such protected health information may be disclosed.

(iii) *No application after release.* For the purposes of this provision, an individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody.

(6) *Covered entities that are government programs providing public benefits.* (i) A health plan that is a government program providing public benefits may disclose protected health information relating to eligibility for or enrollment in the health plan to another agency administering a government program providing public benefits if the sharing of eligibility or enrollment information among such government agencies or the maintenance of such information in a single or combined data system accessible to all such government agencies is required or expressly authorized by statute or regulation.

(ii) A covered entity that is a government agency administering a government program providing public benefits may disclose protected health information relating to the program to another covered entity that is a government agency administering a government program providing public benefits if the programs serve the same or similar populations and the disclosure of protected health information is necessary to coordinate the covered functions of such programs or to improve administration and management relating to the covered functions of such programs.

(l) *Standard: Disclosures for workers' compensation.* A covered entity may disclose protected health information as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

§ 164.514 Other requirements relating to uses and disclosures of protected health information.

(a) *Standard: de-identification of protected health information.* Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.

(b) *Implementation specifications: requirements for de-identification of protected health information.* A covered entity may determine that health information is not individually identifiable health information only if:

(1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

(i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and

(ii) Documents the methods and results of the analysis that justify such determination; or

(2)(i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

(A) Names;

(B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

(*1*) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

(*2*) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

(C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

(D) Telephone numbers;

(E) Fax numbers;

(F) Electronic mail addresses;

(G) Social security numbers;

(H) Medical record numbers;

(I) Health plan beneficiary numbers;

(J) Account numbers;

(K) Certificate/license numbers;

(L) Vehicle identifiers and serial numbers, including license plate numbers;

(M) Device identifiers and serial numbers;

(N) Web Universal Resource Locators (URLs);

(O) Internet Protocol (IP) address numbers;

(P) Biometric identifiers, including finger and voice prints;

(Q) Full face photographic images and any comparable images; and

(R) Any other unique identifying number, characteristic, or code; and

(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

(c) *Implementation specifications: re-identification.* A covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity, provided that:

(1) *Derivation.* The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and

(2) *Security.* The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

(d)(1) *Standard: minimum necessary requirements.* A covered entity must reasonably ensure that the standards, requirements, and implementation specifications of § 164.502(b) and this section relating to a request for or the use and disclosure of the minimum necessary protected health information are met.

(2) *Implementation specifications: minimum necessary uses of protected health information.* (i) A covered entity must identify:

(A) Those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and

(B) For each such person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access.

(ii) A covered entity must make reasonable efforts to limit the access of such persons or classes identified in paragraph (d)(2)(i)(A) of this section to protected health information consistent with paragraph (d)(2)(i)(B) of this section.

(3) *Implementation specification: Minimum necessary disclosures of protected health information.* (i) For any type of disclosure that it makes on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

(ii) For all other disclosures, a covered entity must:

(A) Develop criteria designed to limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought; and

(B) Review requests for disclosure on an individual basis in accordance with such criteria.

(iii) A covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:

(A) Making disclosures to public officials that are permitted under § 164.512, if the public official represents that the information requested is the minimum necessary for the stated purpose(s);

(B) The information is requested by another covered entity;

(C) The information is requested by a professional who is a member of its workforce or is a business associate of the covered entity for the purpose of providing professional services to the covered entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or

(D) Documentation or representations that comply with the applicable requirements of § 164.512(i) have been provided by a person requesting the information for research purposes.

(4) *Implementation specifications: Minimum necessary requests for protected health information.* (i) A covered entity must limit any request for protected health information to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities.

(ii) For a request that is made on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

(iii) For all other requests, a covered entity must review the request on an individual basis to determine that the protected health information sought is limited to the information reasonably necessary to accomplish the purpose for which the request is made.

(5) *Implementation specification: Other content requirement.* For all uses, disclosures, or requests to which the requirements in paragraph (d) of this section apply, a covered entity may not use, discloses or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

(e)(1) *Standard: Uses and disclosures of protected health information for marketing.* A covered entity may not use or disclose protected health information for marketing without an authorization that meets the applicable requirements of § 164.508, except as provided for by paragraph (e)(2) of this section.

(2) *Implementation specifications: Requirements relating to marketing.* (i) A covered entity is not required to obtain an authorization under § 164.508 when it uses or discloses protected health information to make a marketing communication to an individual that:

(A) Occurs in a face-to-face encounter with the individual;

(B) Concerns products or services of nominal value; or

(C) Concerns the health-related products and services of the covered entity or of a third party and the communication meets the applicable conditions in paragraph (e)(3) of this section.

(ii) A covered entity may disclose protected health information for purposes of such communications only to a business associate that assists the covered entity with such communications.

(3) *Implementation specifications: Requirements for certain marketing communications.* For a marketing communication to qualify under paragraph (e)(2)(i) of this section, the following conditions must be met:

(i) The communication must:

(A) Identify the covered entity as the party making the communication;

(B) If the covered entity has received or will receive direct or indirect remuneration for making the communication, prominently state that fact; and

(C) Except when the communication is contained in a newsletter or similar type of general communication device that the covered entity distributes to a broad cross-section of patients, enrollees, or other broad groups of individuals, contain instructions describing how the individual may opt out of receiving future such communications.

(ii) If the covered entity uses or discloses protected health information to target the communication to individuals based on their health status or condition:

(A) The covered entity must make a determination prior to making the communication that the product or service being marketed may be beneficial to the health of the type or class of individual targeted; and

(B) The communication must explain why the individual has been targeted

and how the product or service relates to the health of the individual.

(iii) The covered entity must make reasonable efforts to ensure that individuals who decide to opt out of receiving future marketing communications, under paragraph (e)(3)(i)(C) of this section, are not sent such communications.

(f)(1) *Standard: Uses and disclosures for fundraising.* A covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization meeting the requirements of § 164.508:

(i) Demographic information relating to an individual; and

(ii) Dates of health care provided to an individual.

(2) *Implementation specifications: Fundraising requirements.* (i) The covered entity may not use or disclose protected health information for fundraising purposes as otherwise permitted by paragraph (f)(1) of this section unless a statement required by § 164.520(b)(1)(iii)(B) is included in the covered entity's notice;

(ii) The covered entity must include in any fundraising materials it sends to an individual under this paragraph a description of how the individual may opt out of receiving any further fundraising communications.

(iii) The covered entity must make reasonable efforts to ensure that individuals who decide to opt out of receiving future fundraising communications are not sent such communications.

(g) *Standard: Uses and disclosures for underwriting and related purposes.* If a health plan receives protected heath information for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may not use or disclose such protected health information for any other purpose, except as may be required by law.

(h)(1) *Standard: Verification requirements.* Prior to any disclosure permitted by this subpart, a covered entity must:

(i) Except with respect to disclosures under § 164.510, verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information under this subpart, if the identity or any such authority of such person is not known to the covered entity; and

(ii) Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation, statement, or representation is a condition of the disclosure under this subpart.

(2) *Implementation specifications: Verification.* (i) *Conditions on disclosures.* If a disclosure is conditioned by this subpart on particular documentation, statements, or representations from the person requesting the protected health information, a covered entity may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements.

(A) The conditions in § 164.512(f)(1)(ii)(C) may be satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met.

(B) The documentation required by § 164.512(i)(2) may be satisfied by one or more written statements, provided that each is appropriately dated and signed in accordance with § 164.512(i)(2)(i) and (v).

(ii) *Identity of public officials.* A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:

(A) If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;

(B) If the request is in writing, the request is on the appropriate government letterhead; or

(C) If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

(iii) *Authority of public officials.* A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:

(A) A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority;

(B) If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

(iv) *Exercise of professional judgment.* The verification requirements of this paragraph are met if the covered entity relies on the exercise of professional judgment in making a use or disclosure in accordance with § 164.510 or acts on a good faith belief in making a disclosure in accordance with § 164.512(j).

§ 164.520 Notice of privacy practices for protected health information.

(a) *Standard: notice of privacy practices.* (1) *Right to notice.* Except as provided by paragraph (a)(2) or (3) of this section, an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information.

(2) *Exception for group health plans.* (i) An individual enrolled in a group health plan has a right to notice:

(A) From the group health plan, if, and to the extent that, such an individual does not receive health benefits under the group health plan through an insurance contract with a health insurance issuer or HMO; or

(B) From the health insurance issuer or HMO with respect to the group health plan through which such individuals receive their health benefits under the group health plan.

(ii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and that creates or receives protected health information in addition to summary health information as defined in § 164.504(a) or information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, must:

(A) Maintain a notice under this section; and

(B) Provide such notice upon request to any person. The provisions of paragraph (c)(1) of this section do not apply to such group health plan.

(iii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and does not create or receive protected health information other than summary health information as defined in § 164.504(a) or information on whether an individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, is not required to maintain or provide a notice under this section.

(3) *Exception for inmates.* An inmate does not have a right to notice under this section, and the requirements of this section do not apply to a correctional institution that is a covered entity.

(b) *Implementation specifications: content of notice.*

(1) *Required elements.* The covered entity must provide a notice that is written in plain language and that contains the elements required by this paragraph.

(i) *Header.* The notice must contain the following statement as a header or otherwise prominently displayed: ''THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.''

(ii) *Uses and disclosures.* The notice must contain:

(A) A description, including at least one example, of the types of uses and disclosures that the covered entity is permitted by this subpart to make for each of the following purposes: treatment, payment, and health care operations.

(B) A description of each of the other purposes for which the covered entity is permitted or required by this subpart to use or disclose protected health information without the individual's written consent or authorization.

(C) If a use or disclosure for any purpose described in paragraphs (b)(1)(ii)(A) or (B) of this section is prohibited or materially limited by other applicable law, the description of such use or disclosure must reflect the more stringent law as defined in § 160.202 of this subchapter.

(D) For each purpose described in paragraph (b)(1)(ii)(A) or (B) of this section, the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by this subpart and other applicable law.

(E) A statement that other uses and disclosures will be made only with the individual's written authorization and that the individual may revoke such authorization as provided by § 164.508(b)(5).

(iii) *Separate statements for certain uses or disclosures.* If the covered entity intends to engage in any of the following activities, the description required by paragraph (b)(1)(ii)(A) of this section must include a separate statement, as applicable, that:

(A) The covered entity may contact the individual to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to the individual;

(B) The covered entity may contact the individual to raise funds for the covered entity; or

(C) A group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the sponsor of the plan.

(iv) *Individual rights.* The notice must contain a statement of the individual's rights with respect to protected health information and a brief description of how the individual may exercise these rights, as follows:

(A) The right to request restrictions on certain uses and disclosures of protected health information as provided by § 164.522(a), including a statement that the covered entity is not required to agree to a requested restriction;

(B) The right to receive confidential communications of protected health information as provided by § 164.522(b), as applicable;

(C) The right to inspect and copy protected health information as provided by § 164.524;

(D) The right to amend protected health information as provided by § 164.526;

(E) The right to receive an accounting of disclosures of protected health information as provided by § 164.528; and

(F) The right of an individual, including an individual who has agreed to receive the notice electronically in accordance with paragraph (c)(3) of this section, to obtain a paper copy of the notice from the covered entity upon request.

(v) *Covered entity's duties.* The notice must contain:

(A) A statement that the covered entity is required by law to maintain the privacy of protected health information and to provide individuals with notice of its legal duties and privacy practices with respect to protected health information;

(B) A statement that the covered entity is required to abide by the terms of the notice currently in effect; and

(C) For the covered entity to apply a change in a privacy practice that is described in the notice to protected health information that the covered entity created or received prior to issuing a revised notice, in accordance with § 164.530(i)(2)(ii), a statement that it reserves the right to change the terms of its notice and to make the new notice provisions effective for all protected health information that it maintains. The statement must also describe how it will provide individuals with a revised notice.

(vi) *Complaints.* The notice must contain a statement that individuals may complain to the covered entity and to the Secretary if they believe their privacy rights have been violated, a brief description of how the individual may file a complaint with the covered entity, and a statement that the individual will not be retaliated against for filing a complaint.

(vii) *Contact.* The notice must contain the name, or title, and telephone number of a person or office to contact for further information as required by § 164.530(a)(1)(ii).

(viii) *Effective date.* The notice must contain the date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published.

(2) *Optional elements.* (i) In addition to the information required by paragraph (b)(1) of this section, if a covered entity elects to limit the uses or disclosures that it is permitted to make under this subpart, the covered entity may describe its more limited uses or disclosures in its notice, provided that the covered entity may not include in its notice a limitation affecting its right to make a use or disclosure that is required by law or permitted by § 164.512(j)(1)(i).

(ii) For the covered entity to apply a change in its more limited uses and disclosures to protected health information created or received prior to issuing a revised notice, in accordance with § 164.530(i)(2)(ii), the notice must include the statements required by paragraph (b)(1)(v)(C) of this section.

(3) *Revisions to the notice.* The covered entity must promptly revise and distribute its notice whenever there is a material change to the uses or disclosures, the individual's rights, the covered entity's legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the notice in which such material change is reflected.

(c) *Implementation specifications: Provision of notice.* A covered entity must make the notice required by this

section available on request to any person and to individuals as specified in paragraphs (c)(1) through (c)(4) of this section, as applicable.

(1) *Specific requirements for health plans.* (i) A health plan must provide notice:

(A) No later than the compliance date for the health plan, to individuals then covered by the plan;

(B) Thereafter, at the time of enrollment, to individuals who are new enrollees; and

(C) Within 60 days of a material revision to the notice, to individuals then covered by the plan.

(ii) No less frequently than once every three years, the health plan must notify individuals then covered by the plan of the availability of the notice and how to obtain the notice.

(iii) The health plan satisfies the requirements of paragraph (c)(1) of this section if notice is provided to the named insured of a policy under which coverage is provided to the named insured and one or more dependents.

(iv) If a health plan has more than one notice, it satisfies the requirements of paragraph (c)(1) of this section by providing the notice that is relevant to the individual or other person requesting the notice.

(2) *Specific requirements for certain covered health care providers.* A covered health care provider that has a direct treatment relationship with an individual must:

(i) Provide the notice no later than the date of the first service delivery, including service delivered electronically, to such individual after the compliance date for the covered health care provider;

(ii) If the covered health care provider maintains a physical service delivery site:

(A) Have the notice available at the service delivery site for individuals to request to take with them; and

(B) Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider to be able to read the notice; and

(iii) Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision and promptly comply with the requirements of paragraph (c)(2)(ii) of this section, if applicable.

(3) *Specific requirements for electronic notice.* (i) A covered entity that maintains a web site that provides information about the covered entity's customer services or benefits must prominently post its notice on the web site and make the notice available electronically through the web site.

(ii) A covered entity may provide the notice required by this section to an individual by e-mail, if the individual agrees to electronic notice and such agreement has not been withdrawn. If the covered entity knows that the e-mail transmission has failed, a paper copy of the notice must be provided to the individual. Provision of electronic notice by the covered entity will satisfy the provision requirements of paragraph (c) of this section when timely made in accordance with paragraph (c)(1) or (2) of this section.

(iii) For purposes of paragraph (c)(2)(i) of this section, if the first service delivery to an individual is delivered electronically, the covered health care provider must provide electronic notice automatically and contemporaneously in response to the individual's first request for service.

(iv) The individual who is the recipient of electronic notice retains the right to obtain a paper copy of the notice from a covered entity upon request.

(d) *Implementation specifications: Joint notice by separate covered entities.* Covered entities that participate in organized health care arrangements may comply with this section by a joint notice, provided that:

(1) The covered entities participating in the organized health care arrangement agree to abide by the terms of the notice with respect to protected health information created or received by the covered entity as part of its participation in the organized health care arrangement;

(2) The joint notice meets the implementation specifications in paragraph (b) of this section, except that the statements required by this section may be altered to reflect the fact that the notice covers more than one covered entity; and

(i) Describes with reasonable specificity the covered entities, or class of entities, to which the joint notice applies;

(ii) Describes with reasonable specificity the service delivery sites, or classes of service delivery sites, to which the joint notice applies; and

(iii) If applicable, states that the covered entities participating in the organized health care arrangement will share protected health information with each other, as necessary to carry out treatment, payment, or health care operations relating to the organized health care arrangement.

(3) The covered entities included in the joint notice must provide the notice to individuals in accordance with the applicable implementation specifications of paragraph (c) of this section. Provision of the joint notice to an individual by any one of the covered entities included in the joint notice will satisfy the provision requirement of paragraph (c) of this section with respect to all others covered by the joint notice.

(e) *Implementation specifications: Documentation.* A covered entity must document compliance with the notice requirements by retaining copies of the notices issued by the covered entity as required by § 164.530(j).

§ 164.522 Rights to request privacy protection for protected health information.

(a)(1) *Standard: Right of an individual to request restriction of uses and disclosures.* (i) A covered entity must permit an individual to request that the covered entity restrict:

(A) Uses or disclosures of protected health information about the individual to carry out treatment, payment, or health care operations; and

(B) Disclosures permitted under § 164.510(b).

(ii) A covered entity is not required to agree to a restriction.

(iii) A covered entity that agrees to a restriction under paragraph (a)(1)(i) of this section may not use or disclose protected health information in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted protected health information is needed to provide the emergency treatment, the covered entity may use the restricted protected health information, or may disclose such information to a health care provider, to provide such treatment to the individual.

(iv) If restricted protected health information is disclosed to a health care provider for emergency treatment under paragraph (a)(1)(iii) of this section, the covered entity must request that such health care provider not further use or disclose the information.

(v) A restriction agreed to by a covered entity under paragraph (a) of this section, is not effective under this subpart to prevent uses or disclosures permitted or required under §§ 164.502(a)(2)(i), 164.510(a) or 164.512.

(2) *Implementation specifications: Terminating a restriction.* A covered entity may terminate its agreement to a restriction, if :

(i) The individual agrees to or requests the termination in writing;

(ii) The individual orally agrees to the termination and the oral agreement is documented; or

(iii) The covered entity informs the individual that it is terminating its

agreement to a restriction, except that such termination is only effective with respect to protected health information created or received after it has so informed the individual.

(3) *Implementation specification: Documentation.* A covered entity that agrees to a restriction must document the restriction in accordance with § 164.530(j).

(b)(1) *Standard: Confidential communications requirements.* (i) A covered health care provider must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations.

(ii) A health plan must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the health plan by alternative means or at alternative locations, if the individual clearly states that the disclosure of all or part of that information could endanger the individual.

(2) *Implementation specifications: Conditions on providing confidential communications.*

(i) A covered entity may require the individual to make a request for a confidential communication described in paragraph (b)(1) of this section in writing.

(ii) A covered entity may condition the provision of a reasonable accommodation on:

(A) When appropriate, information as to how payment, if any, will be handled; and

(B) Specification of an alternative address or other method of contact.

(iii) A covered health care provider may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

(iv) A health plan may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.

§ 164.524 Access of individuals to protected health information.

(a) *Standard: Access to protected health information.* (1) *Right of access.* Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, except for:

(i) Psychotherapy notes;

(ii) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and

(iii) Protected health information maintained by a covered entity that is:

(A) Subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a, to the extent the provision of access to the individual would be prohibited by law; or

(B) Exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR 493.3(a)(2).

(2) *Unreviewable grounds for denial.* A covered entity may deny an individual access without providing the individual an opportunity for review, in the following circumstances.

(i) The protected health information is excepted from the right of access by paragraph (a)(1) of this section.

(ii) A covered entity that is a correctional institution or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of protected health information, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.

(iii) An individual's access to protected health information created or obtained by a covered health care provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.

(iv) An individual's access to protected health information that is contained in records that are subject to the Privacy Act, 5 U.S.C. 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law.

(v) An individual's access may be denied if the protected health information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

(3) *Reviewable grounds for denial.* A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed, as required by paragraph (a)(4) of this section, in the following circumstances:

(i) A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;

(ii) The protected health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or

(iii) The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

(4) *Review of a denial of access.* If access is denied on a ground permitted under paragraph (a)(3) of this section, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny. The covered entity must provide or deny access in accordance with the determination of the reviewing official under paragraph (d)(4) of this section.

(b) *Implementation specifications: requests for access and timely action.* (1) *Individual's request for access.* The covered entity must permit an individual to request access to inspect or to obtain a copy of the protected health information about the individual that is maintained in a designated record set. The covered entity may require individuals to make requests for access in writing, provided that it informs individuals of such a requirement.

(2) *Timely action by the covered entity.* (i) Except as provided in paragraph (b)(2)(ii) of this section, the covered entity must act on a request for access no later than 30 days after receipt of the request as follows.

(A) If the covered entity grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested, in accordance with paragraph (c) of this section.

(B) If the covered entity denies the request, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d) of this section.

(ii) If the request for access is for protected health information that is not maintained or accessible to the covered entity on-site, the covered entity must take an action required by paragraph (b)(2)(i) of this section by no later than 60 days from the receipt of such a request.

(iii) If the covered entity is unable to take an action required by paragraph (b)(2)(i)(A) or (B) of this section within the time required by paragraph (b)(2)(i) or (ii) of this section, as applicable, the covered entity may extend the time for such actions by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) or (ii) of this section, as applicable, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request for access.

(c) *Implementation specifications: Provision of access.* If the covered entity provides an individual with access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

(1) *Providing the access requested.* The covered entity must provide the access requested by individuals, including inspection or obtaining a copy, or both, of the protected health information about them in designated record sets. If the same protected health information that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the covered entity need only produce the protected health information once in response to a request for access.

(2) *Form of access requested.* (i) The covered entity must provide the individual with access to the protected health information in the form or format requested by the individual, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form or format as agreed to by the covered entity and the individual.

(ii) The covered entity may provide the individual with a summary of the protected health information requested, in lieu of providing access to the protected health information or may provide an explanation of the protected health information to which access has been provided, if:

(A) The individual agrees in advance to such a summary or explanation; and

(B) The individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation.

(3) *Time and manner of access.* The covered entity must provide the access as requested by the individual in a timely manner as required by paragraph (b)(2) of this section, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy of the protected health information at the individual's request. The covered entity may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.

(4) *Fees.* If the individual requests a copy of the protected health information or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:

(i) Copying, including the cost of supplies for and labor of copying, the protected health information requested by the individual;

(ii) Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and

(iii) Preparing an explanation or summary of the protected health information, if agreed to by the individual as required by paragraph (c)(2)(ii) of this section.

(d) *Implementation specifications: Denial of access.* If the covered entity denies access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

(1) *Making other information accessible.* The covered entity must, to the extent possible, give the individual access to any other protected health information requested, after excluding the protected health information as to which the covered entity has a ground to deny access.

(2) *Denial.* The covered entity must provide a timely, written denial to the individual, in accordance with paragraph (b)(2) of this section. The denial must be in plain language and contain:

(i) The basis for the denial;

(ii) If applicable, a statement of the individual's review rights under paragraph (a)(4) of this section, including a description of how the individual may exercise such review rights; and

(iii) A description of how the individual may complain to the covered entity pursuant to the complaint procedures in § 164.530(d) or to the Secretary pursuant to the procedures in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in § 164.530(a)(1)(ii).

(3) *Other responsibility.* If the covered entity does not maintain the protected health information that is the subject of the individual's request for access, and the covered entity knows where the requested information is maintained, the covered entity must inform the individual where to direct the request for access.

(4) Review of denial requested. If the individual has requested a review of a denial under paragraph (a)(4) of this section, the covered entity must designate a licensed health care professional, who was not directly involved in the denial to review the decision to deny access. The covered entity must promptly refer a request for review to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards in paragraph (a)(3) of this section. The covered entity must promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required by this section to carry out the designated reviewing official's determination.

(e) *Implementation specification: Documentation.* A covered entity must document the following and retain the documentation as required by § 164.530(j):

(1) The designated record sets that are subject to access by individuals; and

(2) The titles of the persons or offices responsible for receiving and processing requests for access by individuals.

§ 164.526 Amendment of protected health information.

(a) *Standard: Right to amend.* (1) *Right to amend.* An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set.

(2) *Denial of amendment.* A covered entity may deny an individual's request for amendment, if it determines that the protected health information or record that is the subject of the request:

(i) Was not created by the covered entity, unless the individual provides a reasonable basis to believe that the

originator of protected health information is no longer available to act on the requested amendment;

(ii) Is not part of the designated record set;

(iii) Would not be available for inspection under § 164.524; or

(iv) Is accurate and complete.

(b) *Implementation specifications: requests for amendment and timely action.* (1) *Individual's request for amendment.* The covered entity must permit an individual to request that the covered entity amend the protected health information maintained in the designated record set. The covered entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment, provided that it informs individuals in advance of such requirements.

(2) *Timely action by the covered entity.* (i) The covered entity must act on the individual's request for an amendment no later than 60 days after receipt of such a request, as follows.

(A) If the covered entity grants the requested amendment, in whole or in part, it must take the actions required by paragraphs (c)(1) and (2) of this section.

(B) If the covered entity denies the requested amendment, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d)(1) of this section.

(ii) If the covered entity is unable to act on the amendment within the time required by paragraph (b)(2)(i) of this section, the covered entity may extend the time for such action by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request for an amendment.

(c) *Implementation specifications: Accepting the amendment.* If the covered entity accepts the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

(1) *Making the amendment.* The covered entity must make the appropriate amendment to the protected health information or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.

(2) *Informing the individual.* In accordance with paragraph (b) of this section, the covered entity must timely inform the individual that the amendment is accepted and obtain the individual's identification of and agreement to have the covered entity notify the relevant persons with which the amendment needs to be shared in accordance with paragraph (c)(3) of this section.

(3) *Informing others.* The covered entity must make reasonable efforts to inform and provide the amendment within a reasonable time to:

(i) Persons identified by the individual as having received protected health information about the individual and needing the amendment; and

(ii) Persons, including business associates, that the covered entity knows have the protected health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

(d) *Implementation specifications: Denying the amendment.* If the covered entity denies the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

(1) *Denial.* The covered entity must provide the individual with a timely, written denial, in accordance with paragraph (b)(2) of this section. The denial must use plain language and contain:

(i) The basis for the denial, in accordance with paragraph (a)(2) of this section;

(ii) The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;

(iii) A statement that, if the individual does not submit a statement of disagreement, the individual may request that the covered entity provide the individual's request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment; and

(iv) A description of how the individual may complain to the covered entity pursuant to the complaint procedures established in § 164.530(d) or to the Secretary pursuant to the procedures established in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in § 164.530(a)(1)(ii).

(2) *Statement of disagreement.* The covered entity must permit the individual to submit to the covered entity a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The covered entity may reasonably limit the length of a statement of disagreement.

(3) *Rebuttal statement.* The covered entity may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the covered entity must provide a copy to the individual who submitted the statement of disagreement.

(4) *Recordkeeping.* The covered entity must, as appropriate, identify the record or protected health information in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the covered entity's denial of the request, the individual's statement of disagreement, if any, and the covered entity's rebuttal, if any, to the designated record set.

(5) *Future disclosures.* (i) If a statement of disagreement has been submitted by the individual, the covered entity must include the material appended in accordance with paragraph (d)(4) of this section, or, at the election of the covered entity, an accurate summary of any such information, with any subsequent disclosure of the protected health information to which the disagreement relates.

(ii) If the individual has not submitted a written statement of disagreement, the covered entity must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the protected health information only if the individual has requested such action in accordance with paragraph (d)(1)(iii) of this section.

(iii) When a subsequent disclosure described in paragraph (d)(5)(i) or (ii) of this section is made using a standard transaction under part 162 of this subchapter that does not permit the additional material to be included with the disclosure, the covered entity may separately transmit the material required by paragraph (d)(5)(i) or (ii) of this section, as applicable, to the recipient of the standard transaction.

(e) *Implementation specification: Actions on notices of amendment.* A covered entity that is informed by another covered entity of an amendment to an individual's protected health information, in accordance with paragraph (c)(3) of this section, must amend the protected health information in designated record sets as provided by paragraph (c)(1) of this section.

(f) *Implementation specification: Documentation.* A covered entity must document the titles of the persons or

offices responsible for receiving and processing requests for amendments by individuals and retain the documentation as required by § 164.530(j).

§ 164.528 Accounting of disclosures of protected health information.

(a) *Standard: Right to an accounting of disclosures of protected health information.* (1) An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures:

(i) To carry out treatment, payment and health care operations as provided in § 164.502;

(ii) To individuals of protected health information about them as provided in § 164.502;

(iii) For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in § 164.510;

(iv) For national security or intelligence purposes as provided in § 164.512(k)(2);

(v) To correctional institutions or law enforcement officials as provided in § 164.512(k)(5); or

(vi) That occurred prior to the compliance date for the covered entity.

(2)(i) The covered entity must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, as provided in § 164.512(d) or (f), respectively, for the time specified by such agency or official, if such agency or official provides the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.

(ii) If the agency or official statement in paragraph (a)(2)(i) of this section is made orally, the covered entity must:

(A) Document the statement, including the identity of the agency or official making the statement;

(B) Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and

(C) Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement pursuant to paragraph (a)(2)(i) of this section is submitted during that time.

(3) An individual may request an accounting of disclosures for a period of time less than six years from the date of the request.

(b) *Implementation specifications: Content of the accounting.* The covered entity must provide the individual with a written accounting that meets the following requirements.

(1) Except as otherwise provided by paragraph (a) of this section, the accounting must include disclosures of protected health information that occurred during the six years (or such shorter time period at the request of the individual as provided in paragraph (a)(3) of this section) prior to the date of the request for an accounting, including disclosures to or by business associates of the covered entity.

(2) The accounting must include for each disclosure:

(i) The date of the disclosure;

(ii) The name of the entity or person who received the protected health information and, if known, the address of such entity or person;

(iii) A brief description of the protected health information disclosed; and

(iv) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure; or, in lieu of such statement:

(A) A copy of the individual's written authorization pursuant to § 164.508; or

(B) A copy of a written request for a disclosure under §§ 164.502(a)(2)(ii) or 164.512, if any.

(3) If, during the period covered by the accounting, the covered entity has made multiple disclosures of protected health information to the same person or entity for a single purpose under §§ 164.502(a)(2)(ii) or 164.512, or pursuant to a single authorization under § 164.508, the accounting may, with respect to such multiple disclosures, provide:

(i) The information required by paragraph (b)(2) of this section for the first disclosure during the accounting period;

(ii) The frequency, periodicity, or number of the disclosures made during the accounting period; and

(iii) The date of the last such disclosure during the accounting period.

(c) *Implementation specifications: Provision of the accounting.* (1) The covered entity must act on the individual's request for an accounting, no later than 60 days after receipt of such a request, as follows.

(i) The covered entity must provide the individual with the accounting requested; or

(ii) If the covered entity is unable to provide the accounting within the time required by paragraph (c)(1) of this section, the covered entity may extend the time to provide the accounting by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (c)(1) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will provide the accounting; and

(B) The covered entity may have only one such extension of time for action on a request for an accounting.

(2) The covered entity must provide the first accounting to an individual in any 12 month period without charge. The covered entity may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period, provided that the covered entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

(d) *Implementation specification: Documentation.* A covered entity must document the following and retain the documentation as required by § 164.530(j):

(1) The information required to be included in an accounting under paragraph (b) of this section for disclosures of protected health information that are subject to an accounting under paragraph (a) of this section;

(2) The written accounting that is provided to the individual under this section; and

(3) The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

§ 164.530 Administrative requirements.

(a)(1) *Standard: Personnel designations.* (i) A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.

(ii) A covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by § 164.520.

(2) *Implementation specification: Personnel designations.* A covered entity must document the personnel designations in paragraph (a)(1) of this section as required by paragraph (j) of this section.

(b)(1) Standard: Training. A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart, as necessary and appropriate for the members of the workforce to

carry out their function within the covered entity.

(2) *Implementation specifications: Training.* (i) A covered entity must provide training that meets the requirements of paragraph (b)(1) of this section, as follows:

(A) To each member of the covered entity's workforce by no later than the compliance date for the covered entity;

(B) Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and

(C) To each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures required by this subpart, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section.

(ii) A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided, as required by paragraph (j) of this section.

(c)(1) *Standard: Safeguards.* A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

(2) *Implementation specification: Safeguards.* A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.

(d)(1) *Standard: Complaints to the covered entity.* A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this subpart or its compliance with such policies and procedures or the requirements of this subpart.

(2) *Implementation specification: Documentation of complaints.* As required by paragraph (j) of this section, a covered entity must document all complaints received, and their disposition, if any.

(e)(1) *Standard: Sanctions.* A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart. This standard does not apply to a member of the covered entity's workforce with respect to actions that are covered by and that meet the conditions of § 164.502(j) or paragraph (g)(2) of this section.

(2) *Implementation specification: Documentation.* As required by paragraph (j) of this section, a covered entity must document the sanctions that are applied, if any.

(f) *Standard: Mitigation.* A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate.

(g) *Standard: Refraining from intimidating or retaliatory acts.* A covered entity may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

(1) *Individuals.* Any individual for the exercise by the individual of any right under, or for participation by the individual in any process established by this subpart, including the filing of a complaint under this section;

(2) *Individuals and others.* Any individual or other person for:

(i) Filing of a complaint with the Secretary under subpart C of part 160 of this subchapter;

(ii) Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Title XI; or

(iii) Opposing any act or practice made unlawful by this subpart, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information in violation of this subpart.

(h) *Standard: Waiver of rights.* A covered entity may not require individuals to waive their rights under § 160.306 of this subchapter or this subpart as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

(i)(1) *Standard: Policies and procedures.* A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart. The policies and procedures must be reasonably designed, taking into account the size of and the type of activities that relate to protected health information undertaken by the covered entity, to ensure such compliance. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirement of this subpart.

(2) *Standard: Changes to policies or procedures.* (i) A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of this subpart;

(ii) When a covered entity changes a privacy practice that is stated in the notice described in § 164.520, and makes corresponding changes to its policies and procedures, it may make the changes effective for protected health information that it created or received prior to the effective date of the notice revision, if the covered entity has, in accordance with § 164.520(b)(1)(v)(C), included in the notice a statement reserving its right to make such a change in its privacy practices; or

(iii) A covered entity may make any other changes to policies and procedures at any time, provided that the changes are documented and implemented in accordance with paragraph (i)(5) of this section.

(3) *Implementation specification: Changes in law.* Whenever there is a change in law that necessitates a change to the covered entity's policies or procedures, the covered entity must promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the notice required by § 164.520, the covered entity must promptly make the appropriate revisions to the notice in accordance with § 164.520(b)(3). Nothing in this paragraph may be used by a covered entity to excuse a failure to comply with the law.

(4) *Implementation specifications: Changes to privacy practices stated in the notice.* (i) To implement a change as provided by paragraph (i)(2)(ii) of this section, a covered entity must:

(A) Ensure that the policy or procedure, as revised to reflect a change in the covered entity's privacy practice as stated in its notice, complies with the standards, requirements, and implementation specifications of this subpart;

(B) Document the policy or procedure, as revised, as required by paragraph (j) of this section; and

(C) Revise the notice as required by § 164.520(b)(3) to state the changed practice and make the revised notice available as required by § 164.520(c). The covered entity may not implement a change to a policy or procedure prior to the effective date of the revised notice.

(ii) If a covered entity has not reserved its right under § 164.520(b)(1)(v)(C) to change a privacy practice that is stated in the notice, the covered entity is bound by the privacy practices as stated

in the notice with respect to protected health information created or received while such notice is in effect. A covered entity may change a privacy practice that is stated in the notice, and the related policies and procedures, without having reserved the right to do so, provided that:

(A) Such change meets the implementation the requirements in paragraphs (i)(4)(i)(A)–(C) of this section; and

(B) Such change is effective only with respect to protected health information created or received after the effective date of the notice.

(5) *Implementation specification: Changes to other policies or procedures.* A covered entity may change, at any time, a policy or procedure that does not materially affect the content of the notice required by § 164.520, provided that:

(i) The policy or procedure, as revised, complies with the standards, requirements, and implementation specifications of this subpart; and

(ii) Prior to the effective date of the change, the policy or procedure, as revised, is documented as required by paragraph (j) of this section.

(j)(1) *Standard: Documentation.* A covered entity must:

(i) Maintain the policies and procedures provided for in paragraph (i) of this section in written or electronic form;

(ii) If a communication is required by this subpart to be in writing, maintain such writing, or an electronic copy, as documentation; and

(iii) If an action, activity, or designation is required by this subpart to be documented, maintain a written or electronic record of such action, activity, or designation.

(2) *Implementation specification: Retention period.* A covered entity must retain the documentation required by paragraph (j)(1) of this section for six years from the date of its creation or the date when it last was in effect, whichever is later.

(k) *Standard: Group health plans.* (1) A group health plan is not subject to the standards or implementation specifications in paragraphs (a) through (f) and (i) of this section, to the extent that:

(i) The group health plan provides health benefits solely through an insurance contract with a health insurance issuer or an HMO; and

(ii) The group health plan does not create or receive protected health information, except for:

(A) Summary health information as defined in § 164.504(a); or

(B) Information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.

(2) A group health plan described in paragraph (k)(1) of this section is subject to the standard and implementation specification in paragraph (j) of this section only with respect to plan documents amended in accordance with § 164.504(f).

§ 164.532 Transition provisions.

(a) *Standard: Effect of prior consents and authorizations.* Notwithstanding other sections of this subpart, a covered entity may continue to use or disclose protected health information pursuant to a consent, authorization, or other express legal permission obtained from an individual permitting the use or disclosure of protected health information that does not comply with §§ 164.506 or 164.508 of this subpart consistent with paragraph (b) of this section.

(b) *Implementation specification: Requirements for retaining effectiveness of prior consents and authorizations.* Notwithstanding other sections of this subpart, the following provisions apply to use or disclosure by a covered entity of protected health information pursuant to a consent, authorization, or other express legal permission obtained from an individual permitting the use or disclosure of protected health information, if the consent, authorization, or other express legal permission was obtained from an individual before the applicable compliance date of this subpart and does not comply with §§ 164.506 or 164.508 of this subpart.

(1) If the consent, authorization, or other express legal permission obtained from an individual permits a use or disclosure for purposes of carrying out treatment, payment, or health care operations, the covered entity may, with respect to protected health information that it created or received before the applicable compliance date of this subpart and to which the consent, authorization, or other express legal permission obtained from an individual applies, use or disclose such information for purposes of carrying out treatment, payment, or health care operations, provided that:

(i) The covered entity does not make any use or disclosure that is expressly excluded from the a consent, authorization, or other express legal permission obtained from an individual; and

(ii) The covered entity complies with all limitations placed by the consent, authorization, or other express legal permission obtained from an individual.

(2) If the consent, authorization, or other express legal permission obtained from an individual specifically permits a use or disclosure for a purpose other than to carry out treatment, payment, or health care operations, the covered entity may, with respect to protected health information that it created or received before the applicable compliance date of this subpart and to which the consent, authorization, or other express legal permission obtained from an individual applies, make such use or disclosure, provided that:

(i) The covered entity does not make any use or disclosure that is expressly excluded from the consent, authorization, or other express legal permission obtained from an individual; and

(ii) The covered entity complies with all limitations placed by the consent, authorization, or other express legal permission obtained from an individual.

(3) In the case of a consent, authorization, or other express legal permission obtained from an individual that identifies a specific research project that includes treatment of individuals:

(i) If the consent, authorization, or other express legal permission obtained from an individual specifically permits a use or disclosure for purposes of the project, the covered entity may, with respect to protected health information that it created or received either before or after the applicable compliance date of this subpart and to which the consent or authorization applies, make such use or disclosure for purposes of that project, provided that the covered entity complies with all limitations placed by the consent, authorization, or other express legal permission obtained from an individual.

(ii) If the consent, authorization, or other express legal permission obtained from an individual is a general consent to participate in the project, and a covered entity is conducting or participating in the research, such covered entity may, with respect to protected health information that it created or received as part of the project before or after the applicable compliance date of this subpart, make a use or disclosure for purposes of that project, provided that the covered entity complies with all limitations placed by the consent, authorization, or other express legal permission obtained from an individual.

(4) If, after the applicable compliance date of this subpart, a covered entity agrees to a restriction requested by an individual under § 164.522(a), a subsequent use or disclosure of

protected health information that is subject to the restriction based on a consent, authorization, or other express legal permission obtained from an individual as given effect by paragraph (b) of this section, must comply with such restriction.

§ 164.534 Compliance dates for initial implementation of the privacy standards.

(a) *Health care providers.* A covered health care provider must comply with the applicable requirements of this subpart no later than February 26, 2003.

(b) *Health plans.* A health plan must comply with the applicable requirements of this subpart no later than the following date, as applicable:

(1) *Health plans other than small health plans*—February 26, 2003.

(2) *Small health plans*—February 26, 2004.

(c) *Health care clearinghouses.* A health care clearinghouse must comply with the applicable requirements of this subpart no later than February 26, 2003.

[FR Doc. 00–32678 Filed 12–20–00; 11:21 am]

BILLING CODE 4150–04–P