Federal Register

Wednesday
November 3, 1999

Part IV

Department of Health and Human Services

Office of the Secretary

45 CFR Parts 160 Through 164

Standards for Privacy of Individually Identifiable Health Information; Proposed Rule

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Parts 160 through 164

RIN 0991–AB08

Standards for Privacy of Individually Identifiable Health Information

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

ACTION: Proposed rule.

SUMMARY: This rule proposes standards to protect the privacy of individually identifiable health information maintained or transmitted in connection with certain administrative and financial transactions. The rules proposed below, which would apply to health plans, health care clearinghouses, and certain health care providers, propose standards with respect to the rights individuals who are the subject of this information should have, procedures for the exercise of those rights, and the authorized and required uses and disclosures of this information.

The use of these standards would 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 would begin to address growing public concerns that advances in electronic technology 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 would implement the privacy requirements of the Administrative Simplification subtitle of the Health Insurance Portability and Accountability Act of 1996.

DATES: Comments will be considered if received as provided below, no later than 5 p.m. on January 3, 2000.

ADDRESSES: Submit electronic comments at the following web site: http://aspe.hhs.gov/admnsimp/.

Mail comments (1 original, 3 copies, and, if possible, a floppy disk) to the following address: U.S. Department of Health and Human Services, Assistant Secretary for Planning and Evaluation, Attention: Privacy-P, Room G–322A, Hubert H. Humphrey Building, 200 Independence Avenue SW, Washington, DC 20201.

If you prefer, you may deliver your written comments (1 original, 3 copies, and, if possible, a floppy disk) to the following address: Room 442E, 200 Independence Avenue, SW, Washington, DC 20201.

See the **SUPPLEMENTARY INFORMATION** section for further information on comment procedures, availability of copies of this document and electronic access to this document.

FOR FURTHER INFORMATION CONTACT: Roxanne Gibson (202) 260–5083.

SUPPLEMENTARY INFORMATION: Comment procedures, availability of copies, and electronic access.

Comment procedures: All comments should include the full name, address and telephone number of the sender or a knowledgeable point of contact. Written comments should include 1 original and 3 copies. If possible, please send an electronic version of the comments on a 3½ inch DOS format floppy disk in Adobe Acrobat Portable Document Format (PDF) (preferred) HTML (preferred), ASCII text, or popular word processor format (Microsoft word, Corel WordPerfect).

Because of staffing and resource limitations, we cannot accept comments by electronic mail or facsimile (FAX) transmission, and all comments and content are to be limited to the 8.5 wide by 11.0 high vertical (also referred to as ''portrait'') page orientation. Additionally, it is requested that if identical/duplicate comment submissions are submitted both electronically and in paper form that each submission clearly indicate that it is a duplicate submission. In each comment, please specify the section of this proposed rule to which the comment applies.

Comments received in a timely fashion will be available for public inspection (by appointment), as they are received, generally beginning approximately three weeks after publication of a document in Room 442E of the Department's offices at 200 Independence Avenue, SW., Washington, DC 20201 on Monday through Friday of each week from 8:30 a.m. to 5 p.m. (phone: 202–260–5083).

After the close of the comment period, comments submitted electronically and written comments that we are technically able to convert will be posted on the Administrative Simplification web site (http://aspe.hhs.gov/admnsimp/).

Copies: To order copies of the **Federal Register** containing this document, send your request to: New Orders, Superintendent of Documents, PO 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
A. Need for privacy standards.
B. Statutory background.
C. Administrative costs.
D. Consultations.
E. Summary and purpose of the proposed rule.
1. Applicability.
2. General rules.
3. Scalability.
4. Uses and disclosures with individual authorization.
5. Uses and disclosures for treatment, payment and health care operations.
6. Permissible uses and disclosures for purposes other than treatment, payment and health care operations.
7. Individual rights.
8. Administrative requirements and policy development and documentation.
9. Preemption.
10. Enforcement.
11. Conclusion.
II. Provisions of the proposed rule.
A. Applicability.
1. Covered entities.
2. Covered information.
3. Interaction with other standards.
4. References to other laws.
B. Definitions.
1. Act.
2. Covered entity.
3. Health care.
4. Health care clearinghouse.
5. Health care provider.
6. Health information.
7. Health plan.
8. Secretary.
9. Small health plan.
10. Standard.
11. State.
12. Transaction.
13. Business partner.
14. Designated record set.
15. Disclosure.
16. Health care operations.
17. Health oversight agency.
18. Individual. 419. Individually identifiable health information.
20. Law enforcement official.
21. Payment.
22. Protected health information.
23. Psychotherapy notes.
24. Public health authority.
25. Research.

26. Research information unrelated to treatment.
27. Treatment.
28. Use.
29. Workforce.
C. General rules.
1. Use and disclosure for treatment, payment, and health care operations.
2. Minimum necessary use and disclosure.
3. Right to restrict uses and disclosures.
4. Creation of de-identified information.
5. Application to business partners.
6. Application to information about deceased persons.
7. Adherence to the notice of information practices.
8. Application to covered entities that are components of organizations that are not covered entities.
D. Uses and disclosures with individual authorization.
1. Requirements when the individual has initiated the authorization.
2. Requirements when the covered entity initiates the authorization.
3. Model forms.
4. Plain language requirement.
5. Prohibition on conditioning treatment or payment.
6. Inclusion in the accounting for uses and disclosures.
7. Revocation of an authorization by the individual.
8. Expired, deficient, or false authorization.
E. Uses and disclosures permitted without individual authorization.
1. Uses and disclosures for public health activities.
2. Use and disclosure for health oversight activities.
3. Use and disclosure for judicial and administrative proceedings.
4. Disclosure to coroners and medical examiners.
5. Disclosure for law enforcement.
6. Uses and disclosure for governmental health data systems.
7. Disclosure of directory information.
8. Disclosure for banking and payment processes.
9. Uses and disclosures for research.
10. Uses and disclosures in emergency circumstances.
11. Disclosure to next-of-kin.
12. Additional uses and disclosures required by other law.
13. Application to specialized classes.
F. Rights of individuals.
1. Rights and procedures for a written notice of information practices.
2. Rights and procedures for access for inspection and copying.
3. Rights and procedures with respect to an accounting of disclosures.
4. Rights and procedures for amendment and correction.
G. Administrative requirements.
1. Designation of a privacy official.
2. Training.
3. Safeguards.
4. Internal complaint process.
5. Sanctions.
6. Duty to mitigate.
H. Development and documentation of policies and procedures.
1. Uses and disclosures of protected health information.
2. Individual requests for restricting uses and disclosures.
3. Notice of information practices.
4. Inspection and copying.
5. Amendment or correction.
6. Accounting for disclosures.
7. Administrative requirements.
8. Record keeping requirements.
I. Relationship to other laws
1. Relationship to State laws.
2. Relationship to other federal laws.
J. Compliance and Enforcement.
1. Compliance
2. Enforcement.
III. Small Business Assistance
1. Notice to individuals of information practices.
2. Access of individuals to protected health information.
3. Accounting for uses and disclosures.
4. Amendment and correction.
5. Designated Privacy official.
6. Training.
7. Safeguards.
8. Complaints.
9. Sanctions.
10. Documentation of policies and procedures.
11. Minimum Necessary.
12. Business partners.
13. Special disclosures that do not require authorization—public health, research, etc.
14. Verification.
IV. Preliminary Regulatory Impact Analysis
A. Relationship of this Analysis to Analyses in Other HIPAA Regulations.
B. Summary of Costs and Benefits.
C. Need for the Proposed Action.
D. Baseline Privacy Protections.
1. Professional Codes of Conduct and the Protection of Health Information.
2. State Laws.
3. Federal Laws.
E. Costs.
F. Benefits.
G. Examination of Alternative Approaches.
1. Creation of de-identified information.
2. General rules.
3. Use and disclosure for treatment, payment, and health care operations.
4. Minimum necessary use and disclosure.
5. Right to restrict uses and disclosures.
6. Application to business partners.
7. Application to information about deceased persons.
8. Uses and disclosures with individual authorization.
9. Uses and disclosures permitted without individual authorization.
10. Clearinghouses and the rights of individuals.
11. Rights and procedures for a written notice of information practices.
12. Rights and procedures for access for inspection and copying.
13. Rights and procedures with respect to an accounting of disclosures.
14. Rights and procedures for amendment and correction.
15. Administrative requirements.
16. Development and documentation of policies and procedures.
17. Compliance and Enforcement.
V. Initial Regulatory Flexibility Analysis
A. Introduction.
B. Economic Effects on Small Entities
1. Number and Types of Small Entities Affected.
2. Activities and Costs Associated with Compliance.
3. The burden on a typical small business.
VI. Unfunded Mandates
A. Future Costs.
B. Particular regions, communities, or industrial sectors.
C. National productivity and economic growth.
D. Full employment and job creation.
E. Exports.
VII. Environmental Impact
VIII. Collection of Information Requirements
IX. Executive Order 12612: Federalism
X. Executive Order 13086: Consultation and Coordination with Indian Tribal Governments
List of Subjects in 45 CFR Parts 160 and 164
Appendix: Sample Provider Notice of Information Practices

I. Background

A. Need for Privacy Standards.

[*Please label comments about this section with the subject: ''Need for privacy standards''*]

The maintenance and exchange of individually identifiable health information is an integral component of the delivery of quality health care. 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. Health care providers, health plans and health care clearinghouses also 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.

Individuals who provide information to health care providers and health plans increasingly are concerned about how their information is used within the health care system. Patients want to know that their sensitive information will be protected not only during the course of their treatment but also in the future as that information is maintained and/or transmitted within and outside of the health care system. Indeed, 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.

Efforts to provide legal protection against the inappropriate use of individually identifiable health

information have been, to date, undertaken primarily by the States. States have adopted a number of laws designed to protect patients against the inappropriate use of health information. A recent survey of these laws indicates, however, that these protections are quite uneven and leave large gaps in their protection. 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).

A clear and consistent set of privacy standards would improve the effectiveness and the efficiency of the 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 expanded use of electronic information has had clear benefits for patients and the health care system as a whole. 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 absence of national standards for the confidentiality of health information has, however, 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. The establishment of a consistent foundation of privacy standards would, therefore, encourage the increased and proper use of electronic information while also protecting the very real needs of patients to safeguard their privacy.

The use of these standards will most clearly benefit patients who are, in increasing numbers, indicating that they are apprehensive about the use and potential use of their health information for inappropriate purposes. A national survey released in January 1999 indicated that one-fifth of Americans already believe that their personal health information has been used inappropriately. See California HealthCare Foundation, ''National Survey: Confidentiality of Medical Records,'' January 1999 (conducted by Princeton Survey Research Associates) (http://www.chcf.org). Of even greater concern, one-sixth of respondents indicated that they had taken some form of action to avoid the misuse of their information, including providing inaccurate information, frequently changing physicians, or avoiding care. The use of these standards will help to restore patient confidence in the health care system, providing benefits to both patients and those who serve them.

In order to administer their plans and provide services, private and public health plans, health care providers, and health care clearinghouses must assure their customers (such as patients, insurers, providers, and health plans) that the health care information they collect, maintain, use, or transmit will remain confidential. The protection of this information is particularly important where it is individually identifiable. Individuals have an important and legitimate interest in the privacy of their health information, and that interest is threatened where there is improper use or disclosure of the information. The risk of improper uses and disclosures has increased as the health care industry has begun to move from primarily paper-based information systems to systems that operate in various electronic forms. The ease of information collection, organization, retention, and exchange made possible by the advances in computer and other electronic technology afford many benefits to the health care industry and patients. At the same time, these advances have reduced or eliminated many of the logistical obstacles that previously served to protect the confidentiality of health information and the privacy interests of individuals.

Congress recognized the need for minimum national health care privacy standards to protect against inappropriate use of individually identifiable health information by passing the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104–191, which called for the enactment of a privacy statute within three years of the date of enactment. The legislation also called for the Secretary of Health and Human Services to develop and send to the Congress recommendations for protecting the confidentiality of health care information, which she did on September 11, 1997. The Congress further recognized the importance of such standards by providing the Secretary of Health and Human Services with authority to promulgate health privacy regulations in lieu of timely action by the Congress. The need for patient privacy protection also was recognized by the President's Advisory Commission on Consumer Protection and Quality in the Health Care Industry in its recommendations for a Consumer Bill of Rights and Responsibilities (November, 1997).

B. Statutory Background.

[*Please label comments about this section with the subject: ''Statutory background''*]

The Congress addressed the opportunities and challenges presented by the health care industry's increasing use of and reliance on electronic technology 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 recognized and 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 electronically in connection with such transactions. HHS proposed such standards in a series of Notices of Proposed Rulemaking (NPRM) published on May 7, 1998 (63 FR 25272 and 25320), and June 16, 1998 (63 FR 32784). At the same time, Congress recognized the challenges to the confidentiality of health information presented by the advances in electronic technology and communication. Section 262 thus also directs HHS to develop standards to protect the security, including the confidentiality and integrity, of such information. HHS issued an NPRM proposing security standards on August 12, 1998 (63 FR 43242).

Congress has recognized that privacy standards must accompany the electronic data interchange standards and that the increased ease of transmitting and sharing individually

identifiable health information must be accompanied by an increase in the privacy and confidentiality. In fact, a significant portion 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 provision. Although the requirement for the issuance of concomitant privacy standards remained as part of the bill passed by the House of Representatives, in conference the requirement for privacy standards was removed from the standard-setting authority of title XI (section 1173 of the Act) and placed in a separate section of HIPAA, section 264. Subsection (b) of section 264 required the Secretary of HHS to develop and submit to the Congress recommendations for:

(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 the Congress on September 11, 1997, and are summarized below. 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 governing standards with respect to the privacy of individually identifiable health information prior to August 21, 1999, HHS has now, in accordance with this statutory mandate, developed proposed rules setting forth standards to protect the privacy of such information.

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.

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 requirements concerning the adoption of standards, including the role of standard setting organizations and required consultations, summarized 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 that are covered, 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. A proposed rule for most of the transactions was published in 1998 with the final rule expected by the end of 1999. The delay was caused by the deliberate consensus building process working with industry and the large number of comments received (about 17,000).

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. We note that these penalties do not affect any other penalties that may be imposed by other federal programs.

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 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 transmitted in connection with the transactions described in section 1173(a)(1). 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.

C. 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.'' As is more fully discussed in the Regulatory Impact and Regulatory Flexibility analyses below, we recognize that the proposed privacy standards would entail substantial initial and ongoing administrative costs for entities subject to the rules. However, as the analyses also indicate, even if the rules proposed below are considered in isolation, they should produce administrative and other cost savings that should more than offset such costs on a national basis. 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, even if the rules proposed below were to impose net costs, which we do not believe they do, they would still be ''consistent with'' the objective of reducing administrative costs for the health care system as a whole.

D. Consultations

[*Please label comments about this section with the subject: ''Consultations''*]

The Congress explicitly 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. In addition we are continuing to consult with this committee by requesting the committee to review this proposed rule and provide comments, and recommendations will be taken into account in developing the final regulation. 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.

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. Relevant federal agencies participated in an interagency working group, 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 group: 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. The interagency working group developed the policies of the proposed rules set forth below.

E. Summary and Purpose of the Proposed Rule

[*Please label comments about this section with the subject: ''Summary and purpose''*]

The following outlines the provisions and operations of this proposed rule and is intended to provide a framework for the following preamble. A more detailed discussion of the authority, rationale, and implementation can be found in Section II of the preamble, Provisions of the Proposed Rule.

As described in more detail in preamble section I.B, above, the HIPAA requires the Secretary of HHS to promulgate a series of standards relating to the electronic exchange of health information. Collectively these are known as the Administrative Simplification provisions. In addition to those standards, the Secretary was required to develop and submit to the Congress recommendations for the privacy 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, and the

uses and disclosures of such information that should be authorized.

On September 11, 1997, the Secretary presented to the Congress her Recommendations for protecting the ''Confidentiality of Individually-Identifiable Health Information'' (the ''Recommendations''), as required by section 264 (a) of HIPAA. In those Recommendations, the Secretary called for new federal legislation to create a national floor of standards that provide fundamental privacy rights for patients, and that define responsibilities for those who use and disclose identifiable health information.

The Recommendations elaborated on the components that should be included in privacy legislation. These components included new restrictions on the use and disclosure of health information, the establishment of new consumer rights, penalties for misuse of information, and redress for those harmed by misuse of their information. The Recommendations served, to the extent possible under the HIPAA legislative authority, as a template for the rules proposed below. They are available on the HHS website at http://aspe.hhs.gov/admnsimp/pvcrec.htm.

The Secretary's Recommendations set forth the a framework for federal privacy legislation. Such legislation should:

- Allow for the smooth flow of identifiable health information for treatment, payment, and related operations, and for specified additional purposes related to health care that are in the public interest.
- Prohibit the flow of identifiable information for any additional purposes, unless specifically and voluntarily authorized by the subject of the information.
- Put in place a set of fair information practices that allow individuals to know who is using their health information, and how it is being used.
- Establish fair information practices that allow individuals to obtain access to their records and request amendment of inaccurate information.
- Require persons who hold identifiable health information to safeguard that information from inappropriate use or disclosure.
- Hold those who use individually identifiable health information accountable for their handling of this information, and to provide legal recourse to persons harmed by misuse.

We believed then, and still believe, that there is an urgent need for legislation to establish comprehensive privacy standards for all those who pay and provide for health care, and those who receive information from them.

This proposed rule implements many of the policies set forth in the Recommendations. However, the HIPAA legislative authority is more limited in scope than the federal statute we recommend, and does not always permit us to propose the policies that we believe are optimal. Our major concerns with the scope of the HIPAA authority include the limited number of entities to whom the proposed rule would be applicable, and the absence of strong enforcement provisions and a private right of action for individuals whose privacy rights are violated.

The Recommendations call for legislation that applies to health care providers and payers who obtain identifiable health information from individuals and, significantly, to those who receive such information from providers and payers. The Recommendations follow health information from initial creation by a health plan or health care provider, through various uses and disclosures, and would establish protections at each step: ''We recommend that everyone in this chain of information handling be covered by the same rules.'' However, the HIPAA limits the application of our proposed rule 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 ''covered entities''). Unfortunately, this leaves many entities that receive, use and disclose protected health information outside of the system of protection that we propose to create.

In particular, the proposed regulation does not directly cover many of the persons who obtain identifiable health information from the covered entities. In this proposed rule we are, therefore, faced with creating new regulatory permissions for covered entities to disclose health information, but cannot directly put in place appropriate restrictions on how many likely recipients of such information may use and re-disclose such information. For example, the Secretary's Recommendations proposed that protected health information obtained by researchers not be further disclosed except for emergency circumstances, for a research project that meets certain conditions, and for oversight of research. In this proposed rule, however, we cannot impose such restrictions. Additional examples of persons who receive this information include workers compensation carriers, researchers, life insurance issuers, employers and marketing firms. We also do not have the authority to directly regulate many of the persons that covered entities hire to perform administrative, legal, accounting, and similar services on their behalf, and who would obtain health information in order to perform their duties. This inability to directly address the information practices of these groups leaves an important gap in the protections provided by the proposed rule.

In addition, only those providers who engage in the electronic administrative simplification transactions can be covered by this rule. Any provider who maintains a solely paper information system would not be subject to these privacy standards, thus leaving another gap in the system of protection we propose to create.

The need to match a regulation limited to a narrow range of covered entities with the reality of information sharing among a wide range of entities leads us to consider limiting the type or scope of the disclosures permitted under this regulation. The disclosures we propose to allow in this rule are, however, necessary for smooth operation of the health care system and for promoting key public goals such as research, public health, and law enforcement. Any limitation on such disclosures could do more harm than good.

Requirements to protect individually identifiable health information must be supported by real and significant penalties for violations. We recommend federal legislation that would include punishment for those who misuse personal health information and redress for people who are harmed by its misuse. We believe there should be criminal penalties (including fines and imprisonment) for obtaining health information under false pretenses, and for knowingly disclosing or using protected health information in violation of the federal privacy law. We also believe that there should be civil monetary penalties for other violations of the law and that any individual whose rights under the law have been violated, whether negligently or knowingly, should be permitted to bring an action for actual damages and equitable relief. Only if we put the force of law behind our rhetoric can we expect people to have confidence that their health information is protected, and ensure that those holding health information will take their responsibilities seriously.

In HIPAA, Congress did not provide such enforcement authority. There is no private right of action for individuals to enforce their rights, and we are concerned that the penalty structure

does not reflect the importance of these privacy protections and the need to maintain individuals' trust in the system. For these and other reasons, we continue to call for federal legislation to ensure that privacy protection for health information will be strong and comprehensive.

1. Applicability

a. *Entities covered.* Under section 1172(a) of the Act, the provisions of this proposed rule apply 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 ''covered entities''). The terms health plan, health care provider, and health care clearinghouse are defined in proposed § 160.103.

As noted above, because we do not have the authority to apply these standards directly to any entity that is not a covered entity, the proposed rule does not directly cover many of the persons who obtain identifiable health information from the covered entities. Examples of persons who receive this information include contractors, third-party administrators, researchers, public health officials, life insurance issuers, employers and marketing firms. We would attempt to fill this gap in our legislative authority in part by requiring covered entities to apply many of the provisions of rule to the entities with whom they contract for administrative and other services. The proposed provision is outlined in more detail below in the discussion of business partners.

b. *Protected health information.* We propose to apply the requirements of this rule to the subset of individual identifiable health information which is maintained or transmitted by covered entities and which is or has been in electronic form. The provisions of the rule would apply to the information itself, referred to as protected health information in this rule, and not to the particular records in which the information is contained. Once information has been 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 it is held by a covered entity).

We understand that our proposal would create a situation in which some health information would be protected while other similar information (e.g., health information contained in paper records that has not been maintained or transmitted electronically) would not be protected. We are concerned about the potential confusion that such a system might entail, but we believe that applying the provisions of the rule to information only in electronic form would result in no real protection for health care consumers. We have requested comment on whether we should extend the scope of the rule to all individually identifiable health information, including purely paper records, maintained by covered entities. Although we are concerned that extending our regulatory coverage to all records might be inconsistent with the intent of the provisions in the HIPAA, we believe that we do have the authority to do so and that there are sound rationale for providing a consistent level of protection to all individually identifiable health information held by covered entities.

2. General Rules

The purpose of our proposal is to define and limit the circumstances in which an individual's protected heath information may be used or disclosed by others. We are proposing to make the use and exchange of protected health information relatively easy for health care purposes, and more difficult for purposes other than health care.

Covered entities would be prohibited from using or disclosing protected health information except as provided in the proposed rule. Under the rule, covered entities could use or disclose protected health information with individual authorization, as provided in proposed § 164.508. Covered entities could use or disclose protected health information without authorization for treatment, payment and health care operations, as provided in § 164.506(a). (The terms ''treatment,'' ''payment'' and ''health care operations'' are defined in proposed § 164.504). Covered entities also would be permitted to use or disclose a patient's protected health information without authorization for specified public and public policy-related purposes, including public health, research, health oversight, law enforcement, and use by coroners, as provided in proposed § 164.510. Covered entities would be permitted to use and disclose protected health information when required to do so by other law, such as mandatory reporting under state law or pursuant to a search warrant.

Covered entities would be required by this rule to disclose protected health information for only two purposes: to permit individuals to inspect and copy protected health information about them, pursuant to proposed § 164.514, and for enforcement of this rule pursuant to proposed § 164.522.

Under our proposal, most uses and disclosures of an individual's protected health information would not require explicit authorization by the individual, but would be restricted by the provisions of the rule. As discussed in section II.C. of this preamble, we propose to substitute regulatory protections for the pro forma authorizations that are used today. The rules would create a sphere of privacy protection that includes covered entities who engage in treatment or payment, and the business partners they hire to assist them. While written consent for these activities would not be required, new restrictions on both internal uses and external disclosures would be put in place to protect the information.

Our proposal is based on the principle that a combination of strict limits on how plans and providers can use and disclose identifiable health information, adequate notice to patients about how such information will be used, and patients' rights to inspect, copy and amend protected health information about them, will provide patients with better privacy protection and more effective control over the dissemination of their information than alternative approaches to patient protection and control.

A central aspect of this proposal is the principle of ''minimum necessary'' disclosure. (See proposed § 164.506(a)). With certain exceptions, permitted uses and disclosures of protected health information would be restricted to the minimum amount of information necessary to accomplish the purpose for which the information is used or disclosed, taking into consideration practical and technological limitations (including the size and nature of the covered entity's business) and costs. While we recognize that there are legitimate uses of protected health information for which patient authorization should not be required, the privilege of this access carries with it an obligation to safeguard the information. Covered entities would be required to take steps to limit the amount of protected health information used or disclosed to the information necessary to meet the purpose of the use or disclosure. These policies could include limiting access to the information to a subset of employees who need to use the information in the course of their work, and limiting the amount of information disclosed from a record to the information needed by the recipient to fulfill the purpose of the disclosure.

We propose that individuals be able to request that a covered entity restrict the protected health information that

results from that encounter (with the exception of encounters for emergency treatment) from further use or disclosure for treatment, payment, and health care operations. (See proposed § 164.506(c)). Covered entities would not be required to agree to restrictions requested by individuals; the rule would only enforce a restriction that has been agreed to by the covered entity and the individual.

Today's health care system is a complex business involving multiple individuals and organizations engaging in a variety of commercial relationships. An individual's privacy should not be compromised when a covered entity engages in such normal business relationships. To accomplish this result, the rule would, with narrow exceptions, require covered entities to ensure that the business partners with which they share protected health information understand—through contract requirements '' that they are subject to standards regarding use and disclosure of protected health information and agree to abide by such rules. (See proposed § 164.506(e)). Other than for purposes of treatment consultation or referral, we would require a contract to exist between the covered entity and the business partner 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 do not intend to interfere with business relationships in the health care industry, but rather to ensure that the privacy of the information shared in these relationships is protected. Business partners would not be permitted to use or disclose protected health information in ways that would not be permitted by the covered entity itself.

3. Scalability

The privacy standards would need to be implemented by all covered entities, from the smallest provider to the largest, multi-state health plan. For this reason, we propose the privacy principles and standards that covered entities must meet, but leave the detailed policies and procedures for meeting these standards to the discretion of each covered entity. We intend that implementation of these standards be flexible and scalable, to account for nature of each covered entity's business, as well as the covered entity's size and resources. A single approach to implementation of these requirements would be neither economically feasible nor effective in safeguarding health information privacy. Instead, we would require that each covered entity assess its own needs and devise and implement privacy policies appropriate to its size, its information practices, and its business requirements. Examples of how implementation of these standards are scalable are provided in the relevant sections of this preamble. (See, also, the discussion in preamble sections II.C. and III.)

4. Uses and Disclosures With Individual Authorization

The rule would require that covered entities have authorization from individuals before using or disclosing their protected health information for any purpose not otherwise recognized by this rule. In § 164.508, we propose rules for obtaining authorizations. Authorizations are needed in a wide array of circumstances. Entities not covered by this rule often want access to individually identifiable health information . For example, a potential employer may require health information as part of a background check for security purposes, or the patient may request a plan or provider to disclose information to obtain eligibility for disability benefits or to an attorney for use in a law suit. Covered entities may also seek such an authorization in order to use protected health information for a purpose not otherwise permitted under this rule. For example, a health plan may wish to use a person's records for developing a marketing strategy.

The proposed authorization requirements are intended to ensure that an individual's authorization is truly voluntary. We would prohibit covered entities from conditioning treatment or payment on the individual agreeing to disclose information for other purposes. We also would require authorizations to clearly and specifically describe the information to be disclosed. If an authorization is sought so that a covered entity may sell, barter, or otherwise exchange the information for purposes other than treatment, payment, or health care operations, the covered entity would have to disclose this fact on the authorization form. We would also require authorizations to be revocable. We do not seek to limit the purposes for which authorization of records disclosure may be sought, but rather to ensure that these authorizations are voluntary, fair, and enforceable.

While the provisions of this proposed rule are intended to make authorizations for treatment and payment purposes unnecessary, some States may continue to require them. This rule would not supersede such State requirements generally, but would impose a new requirement that such State-mandated authorizations must be physically separate from an authorization for other purposes described in this rule.

5. Uses and Disclosures for Treatment, Payment and Health Care Operations

Under this rule, covered entities with limited exceptions would be permitted to use and disclose protected health information without individual authorization for treatment and payment purposes, and for related purposes that we have defined as health care operations. (See § 164.506.) We would construe the terms ''treatment'' and ''payment'' broadly. In section II.B. of this preamble, we describe the types of activities that would be considered health care operations.

6. Permissible Uses and Disclosures for Purposes Other Than Treatment, Payment and Health Care Operations

Individually identifiable health information is needed to support certain national priority activities, such as reducing health care fraud, improving the quality of treatment through research, protecting the public health, and responding to emergency situations. In many cases, the need to obtain authorization for use of health information would create significant obstacles in efforts to fight crime, understand disease, and protect public health. We examined the many uses that the health professions, related industries, and the government make of health information and we are aware of the concerns of privacy and consumer advocates about these uses.

After balancing privacy and other social values, we are proposing rules that would permit use or disclosure of health information without individual authorization for the following national priority activities and activities that allow the health care system to operate smoothly:

- Oversight of the health care system
- Public health functions
- Research
- Judicial and administrative proceedings
- Law enforcement
- Emergency circumstances
- To provide information to next-of-kin
- For identification of the body of a deceased person, or the cause of death
- For government health data systems
- For facility patient directories
- To banks, to process health care payments and premiums
- For management of active duty military and other special classes of individuals

• Where other law requires such disclosure and no other category of permissible disclosures would allow the disclosure

The rule would specify conditions that would need to be met in order for the use or disclosure of protected health information to be permitted for each of these purposes. (See § 164.514) We have proposed conditions tailored to the need for each type of use or disclosure, and to the types of organizations involved in each such activity. These uses and disclosures, and the conditions under which they may occur, are discussed in section II. F of this preamble.

The uses and disclosures that would be permitted under proposed rule would be just that—permissible. Thus, for disclosures that are not compelled by other law, providers and payers would be free to disclose or not, according to their own policies and ethical principles. We propose these rules as a basic set of legal controls, but ethics and professional practice may dictate more guarded disclosure policies. At the same time, nothing in this rule would provide authority for a covered entity to restrict or refuse to make a disclosure mandated by other law.

7. Individual Rights

We are proposing to establish several basic rights for individuals with respect to their protected health information. We propose that individuals be able to obtain access to protected health information about them, which would include a right to inspect and obtain a copy of such information. See proposed § 164.514. The right of access would extend to an accounting of disclosures of the protected health information for purposes other than treatment, payment, and health care operations. See proposed § 164.515.

In § 164.512, we also propose that individuals have a right to receive a written notice of information practices from covered entities. While the primary purpose of this notice would be to inform individuals about the uses and disclosures that a covered entity would intend to make with the information, the notice also would serve to limit the activities of the covered entity—an otherwise lawful use or disclosure that does not appear in the entity's notice would not be permitted. The covered entity's uses and disclosures could be stated in broad terms, but an entity would not be able to make a use or disclosure that is not included in its notice. The covered entity could modify its notice at any time and apply revised practices to existing and new information held by the covered entity.

In addition, we propose that individuals have the right to request amendment or correction of protected health information that is inaccurate or incomplete. See proposed § 164.516. We are proposing procedural requirements and deadlines to implement each of these individual rights.

8. Administrative Requirements and Policy Development and Documentation

In our Recommendations, we call for a federal law that requires holders of identifiable health information to implement safeguards to protect it from inappropriate access, use or disclosure. No legislation or rule can effectively specify how to do this for every holder of health information. But federal rules can and should require those who hold identifiable health information to develop and implement basic administrative procedures to protect that information and protect the rights of the individual with respect to that information.

To accomplish this goal, we propose that covered entities be required to designate a privacy official, develop a privacy training program for employees, implement safeguards to protect health information from intentional or accidental misuse, provide some means for individuals to lodge complaints about the covered entity's information practices, and develop a system of sanctions for employees and business partners who violate the entity's policies or procedures. (See proposed § 164.518.). We also propose, in § 164.520, to require covered entities to maintain documentation of their policies and procedures for complying with the requirements of this proposed rule. The purpose of these requirements is to ensure that covered entities make explicit decisions about who would have access to protected health information, how that information would be used within the entity, and when that information would or would not be disclosed to other entities.

9. Preemption

The 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. The HIPAA also provides that standards issued by the Secretary will not supercede certain other State laws, including: State laws relating to reporting of disease or injury, child abuse, birth or death, public health surveillance, or public health investigation or intervention; State regulatory reporting; State laws which the Secretary finds are necessary to prevent fraud and abuse, to ensure appropriate State regulation of insurance, for State reporting on health care delivery or costs, or for other purposes; or, State laws which the Secretary finds address controlled substances. These provisions are discussed in more detail in preamble section II.I.1.

This proposed rule also must be read in conjunction with other federal laws and regulations that address the use and disclosure of health information. These issues are discussed in preamble section II.I.2.

In general, the rule that we are proposing would create a federal floor of privacy protection, but would not supercede other applicable law that provide greater protection to the confidentiality of health information. In general, our rule would not make entities subject to a state laws to which they are not subject today.

10. Enforcement

The HIPAA grants the Secretary the authority to impose civil monetary penalties against covered entities which fail to comply with the requirements of this rule, and also establishes criminal penalties for certain wrongful disclosures of protected health information. The civil fines are capped at $25,000 for each calendar year for each provision that is violated. The criminal penalties are graduated, increasing if the offense is committed under false pretenses, or with intent to sell the information or reap other personal gain. The statute does not provide for a private right of action for individuals.

We propose to create a complaint system to permit individuals to make complaints to the Secretary about potential violations of this rule. We also propose that covered entities develop a process for receiving complaints from individuals about the entities' privacy practices. (See § 164.522.) Our intent would be to work with covered entities to achieve voluntary compliance with the proposed standards.

11. Conclusion

Although the promise of these proposed standards cannot become reality for many patients because of the gaps in our authority, we believe they would provide important new protections. By placing strict boundaries around the ways covered entities could use and disclose information, these rules would protect health information at its primary sources: health plans and health care providers. By requiring covered entities to inform patients about how their information is being used and

shared, by requiring covered entities to provide access to that information, and by ensuring that authorizations would be truly voluntary, these rules would provide patients with important new tools for understanding and controlling information about them. By requiring covered entities to document their privacy practices, this rule would focus attention on the importance of privacy, and reduce the ways in which privacy is compromised through inattention or misuse.

With the Secretary's recommendations and these proposed rules, we are attempting to further two important goals: to allow the free flow of health information needed to provide and promote high quality health care, while assuring that individuals' health information is properly protected. We seek a balance that permits important uses of information privacy of people who seek care and healing. We believe our Recommendations find that balance, and have attempted to craft this proposed rule to strike that balance as well.

We continue to believe, however, that federal legislation is the best way to guarantee these protections. The HIPAA legislative authority does not allow full implementation of our recommended policies in this proposed rule. The legislation limits the entities that can be held responsible for their use of protected health information, and the ways in which the covered entities can be held accountable. For these and other reasons, we continue to call upon Congress to pass comprehensive federal privacy legislation. Publication of this proposed rule does not diminish our firm conviction that such legislation should be enacted as soon as possible.

II. Provisions of the Proposed Rule

We propose to establish a new subchapter C to title 45 of the Code of Federal Regulations. Although the rules proposed below would only establish two new parts (parts 160 and 164), we anticipate the new subchapter C will eventually contain three parts, part 160, 162, and 164, with parts 161 and 163 being reserved for future expansion, if needed. Part 160 will contain general requirements and provisions applicable to all of the regulations issued under sections 262 and 264 of Public Law 104–191 (the Administrative Simplification provisions of HIPAA). We anticipate that Part 162 will contain the Administrative Simplification regulations relating to transactions, code sets and identifiers. The new part 164 will encompass the rules relating to the security standards authorized by section 1173(d), the electronic signature standard authorized by section 1173(e), and the privacy rules proposed below.

The new part 164 will be composed of two subparts: subparts A and E, with B, C, and D being reserved. Subpart A will consist of general provisions and subpart E will consist of the final privacy rules. Because the new part 160 will apply to the privacy rules, as well as the other Administrative Simplification rules, it is set out below.

A. Applicability

[*Please label comments about this section with the subject: ''Applicability''*]

The discussion below describes the entities and the information that would be subject to the proposed regulation.

1. Covered Entities

The standards in this proposed regulation would apply to all health plans, all health care clearinghouses, and all health care providers that transmit health information in an electronic form in connection with a standard transaction. In this proposed rule, these entities are referred to as ''covered entities.'' See definition at proposed § 160.103.

A health plan is defined by section 1171 to be an individual or group plan that provides for, or pays the cost of, medical care. The statute expressly includes a significant group of employee welfare benefit plans, state-regulated insurance plans, managed care plans, and essentially all government health plans, including Medicare, Medicaid, the veterans health care program, and plans participating in the Federal Employees Health Benefits Program. See discussion of the definition in section II.B.

A health care provider would be a provider of services as defined in section 1861(u) of the Act, 42 U.S.C. 1395x, a provider of medical or other health services as defined in section 1861(s) of the Act, and any other person who furnishes, bills or is paid for health care services or supplies in the normal course of business. See discussion of the definition in section II.B. Health care providers would be subject to the provisions of the rule if they transmit health information in electronic form in connection with a standard transaction. Standard transactions include claims and equivalent encounter information, eligibility and enrollment transactions, premium payments, claims attachments, and others. See proposed § 160.103. Health care providers who themselves do not directly conduct electronic transactions would become subject to the provisions of the proposed rule if another entity, such as a billing agent or hospital, transmits health information in electronic form in connection with a standard transaction on their behalf.

A health care clearinghouse would be a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements. See section 1171(2) of the Act. For purposes of this rule, we would consider billing services, repricing companies, community health management information systems or community health information systems, ''value-added'' networks, switches and similar organizations to be health care clearinghouses for purposes of this part only if they actually perform the same functions as a health care clearinghouse. See discussion of the definition in section II.B.

2. Covered Information

We propose to apply the standards in this proposed regulation to individually identifiable health information that is or has been electronically transmitted or maintained by a covered entity, including such information when it is in non-electronic form (e.g., printed on paper) or discussed orally. In this proposed regulation, such information is referred to as ''protected health information.'' See discussion of the definition in section II.B. Under HIPAA, our authority to promulgate privacy standards extends to all individually identifiable health information, in any form, maintained or transmitted by a covered entity. For reasons discussed below, we are proposing to limit the application of the proposed standards to protected health information. Below we invite comment on whether we should apply the standards to a broader set of individually identifiable health information in the future.

Under the proposal, the standards apply to information, not to specific records. Thus, once protected health information is transmitted or maintained electronically, the protections afforded by this regulation would apply to the information in any form and continue to apply as the information is printed, discussed orally or otherwise changed in form. It would also apply to the original paper version of information that is at some point transmitted electronically. The authority for, and implications of, this scope are discussed in detail in this section, below.

This proposed regulation would not apply to information that has never been electronically maintained or transmitted by a covered entity.

a. *Legislative authority.* Under HIPAA, we have authority to promulgate a

privacy standard that applies to all individually identifiable health information transmitted or maintained by a covered entity, including information in a non-electronic form. We recognize that there may be an expectation that we would apply privacy standards only to information that is electronically maintained and transmitted. Our prior proposals under HIPAA have addressed only electronically maintained and transmitted information. See Notices of Proposed Rulemaking (NPRM) published on May 7, 1998 (63 FR 25272 and 25320), June 16, 1998 (63 FR 32784), and the proposed security standards published on August 12, 1998 (63 FR 43242).

In considering the appropriate reach of the proposed privacy standards, however, we determined that limiting the standards to electronic information would not be consistent with the requirement in HIPAA for the Secretary to address privacy, confidentiality and security concerns relating to individually identifiable health information.

The HIPAA statute, taken as a whole, contemplates an information protection system that assures the privacy, confidentiality and integrity of health information. Two provisions in subtitle F of HIPAA address privacy and confidentiality concerns: section 264, titled ''Recommendations with Respect to Privacy of Certain Health Information'' and section 1173(d), titled ''Security Standards for Health Information.'' See 42 U.S.C. 1320d–1320d–8, enacted as sections 262 and 264 of HIPAA.

In enacting HIPAA, Congress recognized that the increased accessibility of health information made possible by the widespread and growing use of electronic media and the new federal mandate for increased standardization of data, requires enhanced privacy and confidentiality protections. The House Report links privacy and security concerns stating: ''The standards adopted would protect the privacy and confidentiality of health information. Health information is considered relatively ''safe'' today, not because it is secure, but because it is difficult to access. These standards improve access and establish strict privacy protections.'' House Report No. 496, 104th Cong., 2d. Sess., at 99.

Section 264(c) authorizes the Secretary to protect the privacy of individually identifiable health information transmitted in connection with the standard transactions. Section 1173(d) authorizes the Secretary to prescribe requirements that address the security, integrity, and confidentiality of health information maintained or transmitted, in any form or medium, by the covered entities.

Neither the privacy authority in section 264(c) nor the security authority in 1173(d) exclusively limit the scope of protection to electronic information. Section 264(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).'' This statutory language is not on its face limited to electronic transmissions of individually identifiable health information, although electronic transmissions of such information are clearly within its scope. Moreover, the section requires the regulations to address ''at least'' the subjects of the Secretary's Recommendations, which focus on individually identifiable health information, without reference to whether the information is electronic or not.

The security provision also is not limited by its terms to electronically maintained information. Rather, section 1173(d) applies throughout to ''health information,'' a statutorily defined term that clearly covers information in both its electronic and non-electronic forms.

In HIPAA, when Congress intended to limit health information to its electronic form, it did so explicitly. Section 1172(a)(3) of the statute says that the standards apply to health plans and to health care providers who transmit health information *in electronic form* in connection with the standard transactions (emphasis added); by contrast, the section 1173(d) requirements for information maintained or transmitted are not similarly qualified.

Further support for the premise that the standards may reach information that is maintained or transmitted non-electronically is found within section 1173(d) itself. That section explicitly distinguishes within one subsection (§ 1173(d)(1)(A)) between ''record systems used to maintain health information'' and ''*computerized* record systems.'' Thus, the conclusion may be drawn that the record systems covered by the § 1173(d) security standards are intended to include record systems other than those that are exclusively electronic or ''computerized.''

Finally, the section that generally defines the HIPAA standard transactions, section 1173(a), is not limited by its terms to transactions that are electronic. Rather, although all of the transactions described can be performed electronically, all take paper and some take oral forms as well. Indeed, the purpose of the standards, including the security and privacy standards, is stated as ''to enable electronic exchange.'' This purpose would not preclude (and in fact would support) requirements that relate to non-electronic media where they support the overall goal of enabling electronic information exchange. Thus, we believe that the statute authorizes a privacy regulation covering health information in any form or medium maintained or transmitted by the covered entities.

Although we believe that HIPAA authorizes the Secretary to issue regulations covering individually identifiable health information in any form, the proposed privacy standards in this NPRM are directed to protecting only individually identifiable health information that is or at some point has been electronically maintained or transmitted by a covered entity. Those standards do not cover health information that has never been in electronic form.

We are proposing this approach because we believe that it focuses most directly on the primary concern raised by HIPAA: the fact that growing use of computerization in health care, including the rapid growth of electronic transfers of health information, gives rise to a substantial concern about the confidentiality of the health care information that is part of this growing electronic commerce. At the same time, could not adequately address the confidentiality concerns associated with electronic transfers of health information unless we address the resulting uses and disclosures of such information, in whatever form. Indeed, the protection offered by this standard would be devoid of meaning if all non-electronic records and transmissions were excluded. In that event, access to ''protected'' health information would become merely a matter of obtaining the information in a paper or oral form. Such a narrow reading of the statute would lead to a system in which individually identifiable health information transmitted as part of a claim would be protected only until the information was printed or read aloud, at which point protection would disappear. Previously protected information could be freely printed and redistributed, regardless of limits on further electronic redistribution. The statutory language does not compel such an anomalous result.

In developing our proposal, we considered other approaches for determining the information that would be subject to the privacy standards. We

considered but rejected limiting the scope of the proposal to information in electronic form. For the reasons discussed above, such a narrow interpretation would render the standards nearly meaningless. We also considered applying the privacy standards to all individually identifiable health information in any form maintained or transmitted by a covered entity. There are clear advantages to this approach, including permitting covered entities to treat all individually identifiable health information under the same standards. We rejected that approach in favor of our proposed approach which we believe is more focused at the public concerns over health information confidentiality in an electronic communications age. We also were concerned about imposing additional burden with respect to health information that was less likely to present privacy concerns: paper records that are never reduced to electronic form are less likely to become disseminated broadly throughout the health care system. We invite comment on the approach that we are proposing and on whether alternate approaches to determining the health information that would be subject to this regulation would be more appropriate.

We also considered making use of other statutory authorities under which we impose general operating or management conditions for programs (e.g., Medicare, grant programs) to enhance these proposed privacy protections. Doing so could enable us to apply these privacy standards to a wider range of entities than are currently affected, such as health care providers who do not transmit standard transactions electronically. We use many other authorities now to impose confidentiality and privacy requirements, although the current rules lack consistency. It is not clear whether using these other authorities would create more uniform protections or expanded enforcement options. Therefore we request comment on the concept of drawing on other authorities to amplify the protections of these privacy standards.

b. *Application to records containing protected and unprotected health information.* Once transmitted or maintained electronically, protected health information is often mixed with unprotected health information in the same record. For example, under the proposed rules, information from a medical record that is electronically transmitted by a provider to a health plan and then returned to the original record would become protected health information, even though the rest of the information contained in the paper record may not be subject to these privacy rules.

We reiterate that under the proposed rule, the protections would apply to the information itself, not to the particular record in which it is contained or transmitted. Therefore, an entity could not maintain duplicate records and only apply the protections to the information contained in the record that is electronically maintained or transmitted. For example, once an individual's name and diagnostic code is transmitted electronically between covered entities (or business partners), that information must be protected by both the transmitting and receiving entities in every record, written, electronic or other, in which it appears.

We recognize that this approach may require some additional administrative attention to mixed records (records containing protected and unprotected health information) to ensure that the handling of protected health information conforms with these regulations. We considered ways to limit application of these protections to avoid such potential administrative concerns. However, these regulations would have little effect if not applicable to otherwise protected health information simply because it was combined with unprotected health information—any information could be lawfully disclosed simply by including some additional information. Likewise, these regulations would have no meaning if entities could then avoid applying the protections merely by maintaining separate duplicate records. A way to limit these rules to avoid application to mixed information without sacrificing basic protections is not apparent.

Unlike the potential issues inherent in the protection of oral information, there may be relatively simple ways to reduce possible confusion in protecting mixed records. The risk of inappropriate use or disclosure of protected health information in a mixed record can be eliminated simply by handling all information in mixed records as if it were protected. It also may be possible to develop a ''watermark'' analogous to a copyright label, designating which written information is protected. We welcome comments on how best to protect information in mixed records, without creating unnecessary administrative burdens.

Finally, we recognize that these rules may create awkward boundaries and enforcement ambiguities, and seek comment on how best to reduce these ambiguities while maintaining the basic protections mandated by the statute.

3. Interaction With Other Standards

The privacy standards in this proposed regulation would be closely integrated with other standards that have been proposed under the HIPAA Administrative Simplification title. This is particularly true with respect to the proposed security standards published on August 12, 1998 (63 FR 43242).

We understand that we are proposing a broader scope of applicability with respect to covered information under these privacy standards than we have previously proposed under the security standard. We intend to solicit additional comments regarding the scope of information that should be addressed under the security standard in the near future.

We also recognize that in this NPRM we are publishing slightly different definitions for some of the concepts that were defined in previously published NPRMs for the other standards. The differences resulted from the comments received on the previous NPRMs as well as the conceptual work done in the development of this NPRM. As we publish the final rules, we will bring all the definitions into conformance.

4. References to Other Laws

The provisions we propose in this rule would interact with numerous other laws. For example, proposed § 164.510 provides standards for certain uses or disclosures that are permitted in this rule, and in some cases references activities that are authorized by other applicable law, such as federal, State, tribal or territorial laws. In cases where this rule references ''law'' or ''applicable law'' we intend to encompass all applicable laws, decisions, rules, regulations, administrative procedures or other actions having the effect of law. We do not intend to exclude any applicable legal requirements imposed by a governmental body authorized to regulate in a given area. Where particular types of law are at issue, such as in the proposed provisions for preemption of State laws in subpart B of part 160, or permitted disclosures related to the Armed Forces in § 164.510(m), we so indicate by referring to the particular type of law in question (e.g., ''State law'' or ''federal law'').

When we describe an action as ''authorized by law,'' we mean that a legal basis exists for the activity. The phrase ''authorized by law'' is a term of art that includes both actions that are permitted and actions that are required by law. When we specifically discuss an action that is ''required'' or ''mandated,'' we mean that a law compels (or conversely, prohibits) the performance

of the activity in question. For example, in the health oversight context, disclosure of health information pursuant to 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.

B. Definitions. (§§ 160.103 and 164.504)

[*Please label comments about this section with the subject: ''Definitions''*]

Section 1171 of the Act defines several terms and our proposed rules would, for the most part, simply restate the law or adopt definitions previously defined in the other HIPAA proposed rules. In some instances, we propose definitions from the Secretary's Recommendations. We also propose some new definitions for convenience and efficiency of exposition, and others to clarify the application and operation of this rule. We describe the proposed definitions and discuss the rationale behind them, below.

Most of the definitions would be defined in proposed §§ 160.103 and 164.504. The definitions at proposed § 160.103 apply to all Administrative Simplification standards, including this privacy rule and the security standard. The definitions proposed in § 164.504 would apply only to this privacy rule. Certain other definitions are specific to particular sections of the proposed rule and are provided in those sections. The terms that are defined at proposed § 160.103 follow:

1. *Act*. We would define ''Act'' to mean the Social Security Act, as amended. This definition would be added for convenience.

2. *Covered entity*. This definition would be provided for convenience of reference and would 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''). In the preamble we occasionally refer to health plans and the health care providers described above as ''covered plans,'' ''covered providers,'' or ''covered plans and providers.''

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. The provider could not circumvent these requirements by assigning the task to its agent, since the agent would be deemed to be acting as the provider.

3. *Health care*. We would define the term ''health care'' as it is defined in the Secretary's Recommendations. Health care means the provision of care, services, or supplies to a patient and includes 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.

4. *Health care clearinghouse*. We would define ''health care clearinghouse'' as defined by section 1171(2) of the Act. The Act defines a ''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.'' In practice, clearinghouses receive transactions from health care providers, health plans, other health care clearinghouses, or business partners of such entities, and other entities, translate the data from a given format into one acceptable to the entity receiving the transaction, and forward the processed transaction to that entity. There are currently a number of private clearinghouses that contract or perform this function for health care providers. For purposes of this rule, we would consider billing services, repricing companies, community health management information systems or community health information systems, ''value-added'' networks, switches and similar organizations to be health care clearinghouses for purposes of this part only if they actually perform the same functions as a health care clearinghouse.

We would note that we are proposing to exempt clearinghouses from a number of the provisions of this rule that would apply to other covered entities (see §§ 164.512, 164.514 and 164.516 below), because in most cases we do not believe that clearinghouses would be dealing directly with individuals. In many instances, clearinghouses would be considered business partners under this rule and would be bound by their contracts with covered plans and providers. See proposed § 164.506(e). We would adopt this position with the caveat that the exemptions would be void for any clearinghouse that had direct contact with individuals in a capacity other than that of a business partner.

5. *Health care provider*. Section 1171(3) of the Act defines ''health care provider'' as a ''provider of medical services as defined in section 1861(u) of the Act, a provider of medical or other health services as defined in section 1861(s) of the Act, and any other person who furnishes health care services or supplies.'' We are proposing to define ''health care provider'' as the Act does, and clarify that a health care provider is limited to any person or organization that furnishes, bills, or is paid for, health care services or supplies in the normal course of business. This definition would include a researcher who provides health care to the subjects of research, free clinics, and a health clinic or licensed health care professional located at a school or business.

Section 1861(u) of the Act contains the Medicare definition of a provider, which encompasses institutional providers, such as hospitals, skilled nursing facilities, home health agencies, and comprehensive outpatient rehabilitation facilities. Section 1861(s) of the Act defines other Medicare facilities and practitioners, including assorted clinics and centers, physicians, clinical laboratories, various licensed/certified health care practitioners, and suppliers of durable medical equipment. The last portion of the proposed definition encompasses appropriately licensed or certified health care practitioners or organizations, including pharmacies and nursing homes and many types of therapists, technicians, and aides. It also would include any other individual or organization that furnishes health care services or supplies in the normal course of business. An individual or organization that bills and/or is paid for health care services or supplies in the normal course of business, such as a group practice or an ''on-line'' pharmacy accessible on the Internet, is also a health care provider for purposes of this statute.

For a more detailed discussion of the definition of health care provider, we refer the reader to our proposed rule (Standard Health Care Provider Identifier) published on May 7, 1998, in the **Federal Register** (63 FR 25320).

6. *Health information*. We would define ''health information'' as it is defined in section 1171(4) of the Act. ''Health information'' would mean any information, whether oral or recorded in any form or medium, that 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 that 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.

In this paragraph we attempt to clarify the relationship between the defined terms ''health information,'' ''individually identifiable health information'' and ''protected health information.'' The term ''health information'' encompasses the universe of information governed by the administrative simplification requirements of the Act. For example, under section 1173 of the Act, the Secretary is to adopt standards to enable the electronic exchange of all health information. However, protection of personal privacy is primarily a concern for the subset of health information that is ''individually identifiable health information,'' as defined by the Act (see below). For example, a tabulation of the number of students with asthma by school district would be health information, but since it normally could not be used to identify any individuals, it would not usually create privacy concerns. The definition of individually identifiable health information omits some of the persons or organizations that are described as creating or receiving ''health information.'' Some sections of the Act refer specifically to individually identifiable health information, such as section 1177 in setting criminal penalties for wrongful use or disclosure, and section 264 in requesting recommendations for privacy standards. Finally, we propose the phrase ''protected health information'' (§ 164.504) to refer to the subset of individually identifiable health information that is used or disclosed by the entities that are subject to this rule.

7. *Health plan*. We would 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. For clarity, we would incorporate the referenced definitions as currently stated into our proposed definitions.

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 (see section 2791(a) of the Public Health Service Act (PHS Act)). This definition would include, but is not limited to, the 15 types of plans listed in the statute, as well as any combination of them. The term would include, when applied to public benefit programs, the component of the government agency that administers the program. Church plans and government plans are included to the extent that they fall into one or more of the listed categories.

Health plan'' includes the following singly or in combination:

a. ''Group health plan'' (as currently defined by section 2791(a) of the PHS Act). A group health plan is a plan that has 50 or more participants (as the term ''participant'' is currently defined by section 3(7) of ERISA) or is administered by an entity other than the employer that established and maintains the plan. This definition includes both insured and self-insured plans.

Section 2791(a)(1) of the PHS Act defines ''group health plan'' as an employee welfare benefit plan (as defined in current section 3(1) of ERISA) to the extent that the plan provides medical care, including items and services paid for as medical care, to employees or their dependents directly or through insurance, or otherwise.

b. ''Health insurance issuer'' (as currently defined by section 2791(b) of the PHS Act).

Section 2971(b) of the PHS Act defines a ''health insurance issuer'' 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 law that regulates insurance.

c. ''Health maintenance organization'' (as currently defined by section 2791(b) of the PHS Act). Section 2791(b) of the PHS Act currently defines a ''health maintenance organization'' as a federally qualified health maintenance organization, an organization recognized as such 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. These organizations may include preferred provider organizations, provider sponsored organizations, independent practice associations, competitive medical plans, exclusive provider organizations, and foundations for medical care.

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

e. The Medicaid program (title XIX of the Act).

f. A ''Medicare supplemental policy'' as defined under section 1882(g)(1) of the Act. Section 1882(g)(1) of the Act defines a ''Medicare supplemental policy'' as a health insurance policy that a private entity offers a Medicare beneficiary to provide payment for expenses incurred for services and items that are not reimbursed by Medicare because of deductible, coinsurance, or other limitations under Medicare. The statutory definition of a Medicare supplemental policy excludes a number of plans that are similar to Medicare supplemental plans, such as health plans for employees and former employers and for members and former members of trade associations and unions. A number of these health plans may be included under the definitions of ''group health plan'' or ''health insurance issuer,'' as defined in paragraphs ''a'' and ''b'' above.

g. A ''long-term care policy,'' including a nursing-home fixed indemnity policy. A ''long-term care policy'' is considered to be a health plan regardless of how comprehensive it is.

h. 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. This includes plans that are referred to as multiple employer welfare arrangements (''MEWAs'').

i. The health care program for active military personnel under title 10 of the United States Code. See paragraph ''k'', below, for further discussion.

j. The veterans health care program under chapter 17 of title 38 of the United States Code. This health plan primarily furnishes medical care through hospitals and clinics administered by the Department of Veterans Affairs (VA) for veterans enrolled in the VA health care system.

k. The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) as defined in 10 U.S.C. 1072(4). We note that the Act's definition of ''health plan'' omits several types of health care provided by the Department of Defense (DOD). Sections 1171(5)(I) and 1171(5)(K) cover only the health care program for active duty personnel (see 10 U.S.C. 1074(a)) and the CHAMPUS program (see 10 U.S.C. 1079, 1086). What is omitted is health care provided in military treatment facilities to military retirees (see 10 U.S.C. 1074(b)), to dependents of active duty personnel and to dependents of retirees (see 10 U.S.C. 1076), to Secretarial designees such as members of Congress, Justices of the Supreme Court, and to foreign military personnel under NATO status of forces agreements. Health care provided by the DOD in military facilities to the aforementioned persons is not included as a ''health plan'' under HIPAA. However, these facilities would still be considered to be health care providers.

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

seq.). This program furnishes services, generally through its own health care providers, primarily to persons who are eligible to receive services because they are of American Indian or Alaskan Native descent.

m. The Federal Employees Health Benefits Program under 5 U.S.C. chapter 89. This program consists of health insurance plans offered to active and retired federal employees and their dependents. Although section 1171(5)(M) of the Act refers to the ''Federal Employees Health Benefit Plan,'' this and any other rules adopting administrative simplification standards will use the correct name, the Federal Employees Health Benefits Program. One health plan does not cover all federal employees; over 350 health plans provide health benefits coverage to federal employees, retirees, and their eligible family members. Therefore, we will use the correct name, The Federal Employees Health Benefits Program, to make clear that the administrative simplification standards apply to all health plans that participate in the Program.

n. An approved State child health plan for child health assistance that meets the requirements of section 2103 of the Act, which established the Children's Health Insurance Program (CHIP).

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

p. Any other individual plan or group health plan, or combination thereof, that provides or pays for the cost of medical care. 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. Moreover, the statement that the term ''health plan'' ''includes'' the specified plans implies that the term also covers other plans that meet the stated criteria. One approach to interpreting this introductory language in the statute would be to make coverage decisions about plans that may meet these criteria on a case-by-case basis. Instead we propose to clarify its coverage by adding this category to the proposed definition of ''health plan''; we seek public comment on its application. The Secretary would determine which plans that meet the criteria in the preceding paragraph are health plans for purposes of title II of HIPAA.

Consistent with the other parts of HIPAA, the provisions of this rule generally would not apply to 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. 29 U.S.C. 1186(c). We note that health care providers would be subject to the provisions of this rule with respect to the health care they provide to individuals, even if such providers seek or receive reimbursement from an insurance entity that is not a covered entity under these rules. However, nothing in this rule would be intended to prevent a health care provider from disclosing protected health information to a non-covered insurance entity for the purpose of obtaining payment for services. Further, under proposed § 164.510(n), this rule would permit disclosures by health care providers of protected health information to such insurance entities and to other persons when mandated by applicable law for the purposes of determining eligibility for coverage or benefits under such insurance arrangements. For example, a State workers' compensation law that requires disclosure of protected health information to an insurer or employer for the purposes of determining an individual's eligibility for medical or other benefits, or for the purpose of determining fitness for duty, would not be disturbed by this rule.

8. *Secretary.* This term means the Secretary of Health and Human Services and any other officer or employee of the Department of Health and Human Services to whom the authority involved has been delegated. It is provided for ease of reference.

9. *Small health plan.* The HIPAA does not define a ''small health plan,'' but instead explicitly leaves the definition to be determined by the Secretary. We propose to adopt the size classification used by the Small Business Administration. We would therefore define a ''small health plan'' as a health plan with annual receipts of $5 million or less. 31 CFR 121.201. This differs from the definition of ''small health plan'' in prior proposed Administrative Simplification rules. We will conform the definitions in the final Administrative Simplification rules.

10. *Standard.* The term ''standard'' would mean a prescribed set of rules, conditions, or requirements concerning classification of components, specification of materials, performance or operations, or delineation of procedures in describing products, systems, services, or practices. This definition is a general one, to accommodate the varying functions of the specific standards proposed in the other HIPAA regulations, as well as the rules proposed below.

11. *State.* This term would include the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam. This definition follows the statutory definition of ''State'' in section 1101(a) of the Act.

12. *Transaction.* We would define ''transaction,'' as we have done in other Administrative Simplification regulations, to mean the exchange of information between two parties to carry out financial or administrative activities related to health care. A transaction would be (1) any of the transactions listed in section 1173(a)(2) of the Act, and (2) any transaction determined appropriate by the Secretary in accordance with Section 1173(a)(1) of the Act.

A ''transaction'' would mean any of the following:

a. *Health claims or equivalent encounter information.* This transaction could be used to submit health care claim billing information, encounter information, or both, from health care providers to payers, either directly or via intermediary billers and claims clearinghouses.

b. *Health care payment and remittance advice.* This transaction could be used by a health plan to make a payment to a financial institution for a health care provider (sending payment only), to send an explanation of benefits remittance advice directly to a health care provider (sending data only), or to make payment and send an explanation of benefits remittance advice to a health car provider via a financial institution (sending both payment and data).

c. *Coordination of benefits.* This transaction could be used to transmit health care claims and billing payment information between payers with different payment responsibilities where coordination of benefits is required or between payers and regulatory agencies to monitor the furnishing, billing, and/or payment of health care services within a specific health care/insurance industry segment.

d. *Health claims status.* This transaction could be used by health care providers and recipients of health care products or services (or their authorized agents) to request the status of a health care claim or encounter from a health plan.

e. *Enrollment and disenrollment in a health plan.* This transaction could be used to establish communication

between the sponsor of a health benefit and the payer. It provides enrollment data, such as subscriber and dependents, employer information, and primary care health care provider information. A sponsor would be the backer of the coverage, benefit, or product. A sponsor could be an employer, union, government agency, association, or insurance company. The health plan would refer to an entity that pays claims, administers the insurance product or benefit, or both.

f. *Eligibility for a health plan.* This transaction could be used to inquire about the eligibility, coverage, or benefits associated with a benefit plan, employer, plan sponsor, subscriber, or a dependent under the subscriber's policy. It also could be used to communicate information about or changes to eligibility, coverage, or benefits from information sources (such as insurers, sponsors, and payers) to information receivers (such as physicians, hospitals, third party administrators, and government agencies).

g. *Health plan premium payments.* This transaction could be used by, for example, employers, employees, unions, and associations to make and keep track of payments of health plan premiums to their health insurers. This transaction could also be used by a health care provider, acting as liaison for the beneficiary, to make payment to a health insurer for coinsurance, copayments, and deductibles.

h. *Referral certification and authorization.* This transaction could be used to transmit health care service referral information between health care providers, health care providers furnishing services, and payers. It could also be used to obtain authorization for certain health care services from a health plan.

i. *First report of injury.* This transaction could be used to report information pertaining to an injury, illness, or incident to entities interested in the information for statistical, legal, claims, and risk management processing requirements.

j. *Health claims attachments.* This transaction could be used to transmit health care service information, such as subscriber, patient, demographic, diagnosis, or treatment data for the purpose of a request for review, certification, notification, or reporting the outcome of a health care services review.

k. *Other transactions as the Secretary may prescribe by regulation.* Under section 1173(a)(1)(B) of the Act, the Secretary may adopt standards, and data elements for those standards, for other financial and administrative transactions deemed appropriate by the Secretary. These transactions would be consistent with the goals of improving the operation of the health care system and reducing administrative costs.

In addition to the above terms, a number of terms are defined in proposed § 164.504, and are specific to the proposed privacy rules. They are as follows:

13. *Business partner.* This term would mean a person to whom a 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. Such term includes any agent, contractor or other person who receives protected health information from the covered entity (or from another business partner of the covered entity) for the purposes described in the previous sentence. It would not include a person who is an employee, a volunteer or other person associated with the covered entity on a paid or unpaid basis.

14. *Designated record set.* This term would be defined 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. The concept of a ''designated record set'' is derived from the Privacy Act's concept of a ''system of records.'' Under the Privacy Act, federal agencies must provide an individual with access to ''information pertaining to him which is contained in [a system of records].'' 5 U.S.C. 552a(d)(1). A ''system of records'' is defined as ''a group of any records under the control of any agency 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.'' 5 U.S.C. 552a(a)(5). Under this rule, we would substitute the term ''covered entity'' for ''agency'' and limit the information to that used by the covered entity to make decisions about the individual.

We would define a ''record'' as ''any item, collection, or grouping of protected health information maintained, collected, used, or disseminated by a covered entity.'' Under the Privacy Act, ''the term 'record' means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.'' 5 U.S.C. 552a(a)(4). For purposes of this rule we propose to limit the information to protected health information, as defined in this rule. ''Protected health information'' already incorporates the concept of identifiability, and therefore our definition of ''record'' is much simpler.

For health plans, designated record sets would include, at a minimum, the claims adjudication, enrollment, and patient accounting systems. For health care providers, designated record sets would include, at a minimum, the medical records and billing records. Designated record set would also include a correspondence system, a complaint system, or an event tracking system if decisions about individuals are made based, in whole or in part, on information in those systems. Files used to backup a primary data system or the sequential files created to transmit a batch of claims to a clearinghouse are clear examples of data files which would not fall under this definition.

We note that a designated record set would only exist for types of records that a covered entity actually ''retrieves'' by an identifier, and not records that are only ''retrievable'' by an identifier. In many cases, technology will permit sorting and retrieving by a variety of fields and therefore the ''retrievable'' standard would be relatively meaningless.

15. *Disclosure.* This term would be defined as the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

16. *Health care operations.* We propose the term ''health care operations'' to clarify the activities we consider to be ''compatible with and directly related to'' treatment and payment and therefore would not require authorization from the individual for use or disclosure of protected health information.

Under our proposal, ''health care operations'' means the following services or activities if provided by or on behalf of a covered health plan or health care provider for the purposes of carrying out the management functions of such plan or provider necessary for the support of treatment or payment:

- Conducting quality assessment and improvement activities, including evaluating outcomes, and developing clinical guidelines;

- Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which undergraduate and graduate students and trainees in all areas of health care learn under supervision to practice as health care providers (e.g., residency programs, grand rounds, nursing practicums), accreditation, certification, licensing or credentialing activities;
- Insurance rating and other insurance activities relating to the renewal of a contract for insurance, including underwriting, experience rating, and reinsurance, but only when the individuals are already enrolled in the health plan conducting such activities and only when the use or disclosure of such protected health information relates to an existing contract of insurance (including the renewal of such a contract);
- Conducting or arranging for auditing services, including fraud and abuse detection and compliance programs; and
- Compiling and analyzing information in anticipation of, or for use in, civil or criminal legal proceedings.

Our definition proposes to limit health care operations to functions and activities performed by a health plan or provider or by a business partner on behalf of a health plan or a provider. Our definition anticipates that in order for treatment and payment to occur, protected health information would be used within entities, would be shared with business partners, and in some cases would be shared between covered entities (or their business partners). However, a health care operation should not result in protected health information being disclosed to an entity that is not the covered entity (or a business partner of such entity) on whose behalf the operation is being performed. For example, a health plan may request a health care provider to provide protected health information to the health plan, or to a business partner of the health plan, as part of an outcomes evaluation effort relating to providers affiliated with that plan. This would be a health care operation.

We are aware that the health care industry is changing and that these categories, though broad, may need to be modified to reflect different conditions in the future.

17. *Health oversight agency.* We would define the term ''health oversight agency'' as it is defined in the Secretary's Recommendations. See section II.E. below for further discussion.

18. *Individual.* We would define ''individual'' to mean the person who is the subject of protected health information. We would define the term to include, with respect to the signing of authorizations and other rights (such as access, copying, and correction), various types of legal representatives. The term would include court-appointed guardians or persons with a power of attorney, including persons making health care decisions for incapacitated persons, persons acting on behalf of a decedent's estate, where State or other applicable law authorizes such legal representatives to exercise the person's rights in such contexts, and parents subject to certain restrictions explained below. We would define this term to exclude foreign military and foreign diplomatic personnel and their dependents who receive health care provided or paid for by the DOD or other federal agency or entity acting on its behalf, and overseas foreign national beneficiaries of health care provided by the DOD or other federal agency, or non-governmental organization acting on its behalf.

a. *Disclosures pursuant to a power of attorney.* The definition of an individual would include legal representatives, to the extent permitted under State or other applicable law. We considered several issues in making this determination.

A ''power of attorney'' is a legal agreement through which a person formally grants authority to another person to make decisions on the person's behalf about financial, health care, legal, and/or other matters. In granting power of attorney, a person does not give up his or her own right to make decisions regarding the health care, financial, legal, or other issues involved in the legal agreement. Rather, he or she authorizes the other person to make these decisions as well.

In some cases, an individual gives another person power of attorney over issues not directly related to health care (e.g., financial matters) while informally relying on a third person (either implicitly or through verbal agreement) to make health care decisions on his or her behalf. In such situations, the person with power of attorney could seek health information from a health plan or provider in order to complete a task related to his or her power of attorney. For example, a person with financial power of attorney may request health information from a health plan or provider in order to apply for disability benefits on the individual's behalf.

In developing proposed rules to address these situations, we considered two options: (1) Allowing health plans and health care providers to disclose health information without authorization directly to the person with power of attorney over issues not directly related to health care; and (2) prohibiting health plans or health care providers from disclosing health information without authorization directly to such persons and stating that disclosure without authorization is permitted only to persons designated formally (through power of attorney for health care) or informally as the patient's health care decision-maker. We believe that both options have merit.

The first option recognizes that the responsibilities of persons with power of attorney often are broad, and that even when the power of attorney agreement does not relate directly to health care, the person with power of attorney at times has a legitimate need for health information in order to carry out his or her legal responsibility. The second option recognizes that when an individual is competent to make health care decisions, it is appropriate for him or her (or, if the individual wishes, for the informally designated health care decision maker) to decide whether the covered entity should disclose health information to someone with power of attorney over issues not directly related to health care.

In light of the fact that laws vary by State regarding power of attorney and that implementation of either option could be in the individual's interest, we would allow health plans and health care providers to disclose protected health information without authorization directly to persons with power of attorney to handle any issue on the individual's behalf, in accordance with State or other applicable laws regarding this issue.

This definition also accounts for situations in which a competent individual has granted one person power of attorney over health care issues yet, in practice, relies on another person to make health care decisions. We recognize that, by giving power of attorney for health care issues to one person and involving another person informally in making treatment decisions, the individual is, in the first instance, formally granting consent to release his or her health information and, in practice, granting consent to release medical information to the second person. Therefore, we would allow a health plan or provider, pursuant to State or other applicable law, to disclose protected health information without authorization to a person with power of attorney for the patient's health care and to a person

informally designated as the patient's health care decision maker.

b. *Disclosures pertaining to incapacitated individuals.* Covered entities would be permitted to disclose protected health information to any person making health care decisions for an incapacitated person under State or other applicable law. This definition defers to current laws regarding health care decision-making when a patient is not a minor and is incapable of making his or her own decisions. We propose to permit information to follow such decision-making authority. It is our intent not to disturb existing practices regarding incapacitated patients.

Applicable laws vary significantly regarding the categories of persons who can make health care decisions when a patient is incapable of making them. For example, some State laws establish a hierarchy of persons who may make medical decisions for the incapacitated person (e.g., first a person with power of attorney, if not then next-of-kin, if none then close friend, etc.). In other States, health care providers may exercise professional judgment about which person would make health care decisions in the patient's best interest. We also recognize that federal agencies have, in some cases, established rules regarding such patients. For example, the DOD has established requirements regarding military personnel who are based overseas and who have become incapable of making their own decisions.

Because laws vary regarding patients unable to make their own decisions and because these patients' interests could be served through a variety of arrangements, we would allow health plans and health care providers to disclose information in accordance with applicable laws regarding incapacitated patients.

c. *Disclosures pertaining to minors.* In general, because the definition of individual would include parents, a parent, guardian, or person acting *in loco parentis* could exercise the rights established under this regulation on behalf of their minor (as established by applicable law) children. However, in cases where a minor lawfully obtains a health care service without the consent of or notification to a parent, the minor would be treated as the individual for purposes of exercising any rights established under this regulation with respect to protected health information relating to such health services. Laws regarding access to health care for minors and confidentiality of their medical records vary widely; this proposed regulation recognizes and respects the current diversity of the law in this area. It would not affect applicable regulation of the delivery of health care services to minors, and would not preempt any law authorizing or prohibiting disclosure of individually identifiable health information of minor individuals to their parents. The disclosure of individually identifiable health information from substance abuse records is also addressed by additional requirements established under 42 CFR part 2.

d. *Foreign recipients of defense related health care.* We would define the term ''individual'' to exclude foreign military and foreign diplomatic personnel and their dependents who receive health care provided by or paid for by the DOD or other federal agency, or by an entity acting on its behalf, pursuant to a country-to-country agreement or federal statute. We would also exclude from this term overseas foreign national beneficiaries of health care provided by the DOD or other federal agency or by a non-governmental organization acting on behalf of DOD or such agency. This exclusion is discussed in section II.E.l3.

e. *Disclosures pertaining to deceased persons.* This provision is discussed in Section II.C.6.

19. *Individually identifiable health information.* We would define ''individually identifiable health information'' as it is defined in section 1171(6) of the Act. While the definition of individually identifiable health information does not expand on the statutory definition, we recognize that the issue of how the identifying characteristics can be removed from such information (referred to in this rule as de-identification) presents difficult operational issues. Accordingly, we propose in § 164.506(d) an approach for de-identifying identifiable information, along with restrictions designed to ensure that de-identified information is not used inappropriately.

The privacy standards would apply to ''individually identifiable health information,'' and not to information that does not identify the individual. We are aware that, even after removing obvious identifiers, there is always some probability or risk, however remote, that any information about an individual can be attributed. A 1997 MIT study showed that, because of the public availability of the Cambridge, Massachusetts voting list, 97 percent of the individuals in Cambridge whose data appeared in a data base which contained only their nine digit zip code and birth date could be identified with certainty. [1] Their information had been ''de-identified'' (some obvious identifiers had been removed) but it was not anonymous (it was still possible to identify the individual).

It is not always obvious when information identifies the subject. If the name and identifying numbers (e.g., SSN, insurance number, etc.) are removed, a person could still be identified by the address. With the address removed, the subject of a medical record could be identified based on health and demographic characteristics (e.g., age, race, diagnosis). ''Identifiability'' varies with the location of the subject; there could be hundreds of people in Manhattan who have the same age, race, gender, and diagnosis, but only one such person in a small town or rural county. Gauging the risk of identification of information requires statistical experience and expertise that most covered entities will not possess.

Obvious identifiers on health information could be replaced with random numbers or encrypted codes, which can prevent the person using the record from identifying the subject, but which allow the person holding the code to re-identify the information. Information with coded or encrypted identifiers would be considered ''de-identified'' but not ''anonymous,'' because it is still possible for someone to identify the subject.

We considered defining ''individually identifiable health information'' as any information that is not anonymous, that is, for which there is any possibility of identifying the subject. We rejected this option, for several reasons. First, the statute suggests a different approach. The term ''individually identifiable health information'' is defined in HIPAA as health information that ''* * * identifies the individual, or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.'' By including the modifier ''reasonable basis,'' Congress appears to reject the absolute approach to defining ''identifiable.''

Second, covered entities may not have the statistical sophistication to know with certainty when sufficient identifying information has been removed so that the record is no longer identifiable. We believe that covered entities need more concrete guidance as to when information will and will not be ''identifiable'' for purposes of this regulation.

[1] 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.

Finally, defining non-identifiable to mean anonymous would require covered entities to comply with the terms of this regulation with respect to information for which the probability of identification of the subject is very low. We want to encourage covered entities and others to remove obvious identifiers or encrypt them whenever possible; use of the absolute definition of ''identifiable'' would not promote this salutary result.

For these reasons, we propose at § 164.506(d)(2)(ii) that there be a presumption that, if specified identifying information is removed and if the holder has no reason to believe that the remaining information can be used by the reasonably anticipated recipients alone or in combination with other information to identify an individual, then the covered entity is presumed to have created de-identified information.

At the same time, in proposed § 164.506(d)(2)(iii), we would leave leeway for more sophisticated data users to take a different approach. We would include a ''reasonableness'' standard so that entities with sufficient statistical experience and expertise could remove or code a different combination of information, so long as the result is still a low probability of identification. With this approach, our intent is to provide certainty for most covered entities, while not limiting the options of more sophisticated data users.

In § 164.504, we propose to define ''individually identifiable health information'' to mean health information created or received by a health care provider, health plan, employer or health care clearinghouse, that could be used directly or indirectly to identify the individual who is the subject of the information. Under proposed § 164.506(d)(2)(ii), information would be presumed not to be ''identifiable'' if:

- All of the following data elements have been removed or otherwise concealed: Name; address, including street address, city, county, zip code, or equivalent geocodes; names of relatives and employers; birth date; telephone and fax numbers; e-mail addresses; social security number; medical record number; health plan beneficiary number; account number; certificate/license number; any vehicle or other device serial number; web URL; Internet Protocol (IP) address; finger or voice prints; photographic images; and any other unique identifying number, characteristic, or code (whether generally available in the public realm or not) that the covered entity has reason to believe may be available to an anticipated recipient of the information, and
- The covered entity has no reason to believe that any reasonably anticipated recipient of such information could use the information alone, or in combination with other information, to identify an individual. Thus, to create de-identified information, entities that had removed the listed identifiers would still have to remove additional data elements if they had reason to believe that a recipient could use the remaining information, alone or in combination with other information, to identify an individual. For example, if the ''occupation'' field is left intact and the entity knows that a person's occupation is sufficiently unique to allow identification, that field would have to be removed from the relevant record. The presumption does not allow use or disclosure if the covered entity has reason to believe the subject of the information can be re-identified. Our concern with the potential for re-identification is heightened by our limited jurisdiction under HIPAA. Because we can only regulate health care providers, health plans and health care clearinghouses, we cannot prohibit other recipients of de-identified information from attempting to re-identify it.

To assist covered entities in ascertaining whether their attempts to create de-identified information would be successful, the Secretary would from time to time issue guidance establishing methods that covered entities could use to determine the identifiability of information. This guidance would include information on statistical and other tests that could be performed by covered entities in assessing whether they have created de-identified information. The manner in which such guidance would be published and distributed will be addressed in the final regulation. We solicit comment on the best ways in which to inform covered entities of appropriate and useful information on methods that they can use to determine whether information is de-identified.

In enforcing this regulation, the Secretary would consider the sophistication of covered entities when determining whether a covered entity had reason to believe that information that it had attempted to de-identify continued to identify the subject. Covered entities that routinely create and distribute de-identified data would be expected to be aware of and to use advanced statistical techniques, including the guidance issued by the Secretary, to ensure that they are not improperly disclosing individually identifiable health information. Covered entities that rarely create de-identified information would not be expected to have the same level of knowledge of these statistical methods, and generally could rely on the presumption that information from which they have removed the listed identifiers (and provided that they do not know that the information remains identifiable) is de-identified. We solicit comment on whether the enforcement approach that we are suggesting here and our overall approach relating to the creation of de-identified information would provide sufficient guidance to covered entities to permit them to create, use and disclose de-identified information.

In addition, we propose to permit entities with appropriate statistical experience and expertise (obtained through a statistical consultant or staff with statistical expertise) to decide that some of the above named data elements could be retained in the de-identified data set if: (1) The entity determines that the probability of identifying an individual with the remaining information is very low, or (2) the entity has converted the ''identifiable'' data elements into data elements that, in combination with the remaining information, have a very low probability of being used to identify an individual. An example of such a conversion would be the translation of birth date into age expressed in years or, if still determined to convey ''identifiability,'' age expressed in categories of years (e.g., age 18 to 24). In making these determinations, the entity must consider the data elements taken together as well as any additional information that might reasonably be available to a recipient. Examples of the types of entities that would have the statistical experience and expertise to make this type of judgment include large health research institutions such as medical schools with epidemiologists and statisticians on the faculty; federal agencies such as the National Center for Health Statistics, the Agency for Health Care Policy and Research, FDA, the Bureau of the Census, and NIH; and large corporations that do health research such as pharmaceutical manufacturers with epidemiologists and statisticians on staff.

An important component of this approach to defining ''identifiable'' would be the prohibition on re-identification of health information. We propose that a covered entity that is a recipient of de-identified information who attempts to re-identify such de-identified information for a purpose for which protected health information could not be used or disclosed under

this rule be deemed to be in violation of the law. See proposed § 164.506(d) and section II.C. below. There may be circumstances, however, when recipients of de-identified information will have a legitimate reason to request that the de-identified information be re-identified by the originating covered entity. For example, if a researcher received de-identified information from a covered entity and the research revealed that a particular patient was misdiagnosed, the covered entity should be permitted to re-identify the patient's health information so that the patient could be informed of the error and seek appropriate care. One of the principal reasons entities retain information in coded form, rather than rendering it anonymous, is to enable re-identification of the information for appropriate reasons. Although we would anticipate that the need for re-identification would be rare, entities that expect to have to perform this function should establish a process for determining when re-identification is appropriate. Once covered entities re-identify information, it becomes protected information and may, therefore, be used and disclosed only as permitted by this regulation.

The phrase ''individually identifiable'' information is already in use by many HHS agencies and others. In particular, the Common Rule regulation includes ''identifiable private information'' in its definition of ''human subject.'' Because of this, medical records research on ''identifiable private information'' is subject to Common Rule consent and IRB review requirements. It would not be our intent to suggest changes to this practice. Researchers and others can and are encouraged to continue to use more stringent approaches to protecting information.

We invite comment on the approach that we are proposing and on alternative approaches to standards for covered entities to determine when health information can reasonably be considered no longer individually identifiable.

20. *Law enforcement official.* We propose a new definition of ''law enforcement official,'' to mean an officer of the United States or a political subdivision thereof, who is empowered by law to conduct an investigation or official proceeding inquiring into a violation of, or failure to comply with, any law; or a criminal, civil, or administrative proceeding arising from a violation of, or failure to comply with, any law.

21. *Payment.* We offer a new definition of payment. The term ''payment'' would mean activities undertaken by a health plan (or by a business partner on behalf of a health plan) to determine its responsibilities for coverage under the health plan policy or contract including the actual payment under the policy or contract, or by a health care provider (or by a business partner on behalf of a provider) to obtain reimbursement for the provision of health care, including:

- Determinations of coverage, improving payment methodologies or coverage policies, or adjudication or subrogation of claims;
- Risk adjusting payments based on enrollee health status and demographic characteristics;
- Billing, claims management, medical review, medical data processing;
- Review of health care services with respect to medical necessity, coverage under a health plan policy or contract, appropriateness of care, or justification of charges; and,
- Utilization review activities, including pre-certification and preauthorization of services.

Our proposed definition is intended to capture the necessary sharing of protected health information among health care providers who provide care, health plans and other insurers who pay for care, their business partners, as well as sponsors of group health plans, such as employers, who pay for care and sometimes provide administrative services in conjunction with health plan payment activities. For example, employers sometimes maintain the eligibility file with respect to a group health plan.

Our proposed definition anticipates that protected health information would be used for payment purposes within entities, would be shared with business partners, and in most cases would be shared between health care providers and health plans (and their business partners). In some cases, a payment activity could result in the disclosure of protected health information by a plan to an employer or to another payer of health care, or to an insurer that is not a covered entity, such as for coordination of benefits or to a workers compensation carrier. For example, a health plan could disclose protected health information to an employer in connection with determining the experience rate for group coverage.

We are concerned that disclosures for payments may routinely result in disclosures of protected health information to non-covered entities, such as employers, which are not subject to the use and disclosure requirements of this rule. We considered prohibiting disclosures to employers without individual authorization, or alternatively, requiring a contractual relationship, similar to the contracts required for business partners, before such disclosures could occur. We note that the National Committee on Quality Assurance has adopted a standard for the year 2000 that would require health plans to ''have policies that prohibit sending identifiable personal health information to fully insured or self-insured employers and provide safeguards against the use of information in any action relating to an individual'' (Standard R.R.6, National Committee for Quality Assurance 2000 Standards).

We did not adopt either of these approaches, however, because we were concerned that we might disrupt some beneficial activities if we were to prohibit or place significant conditions on disclosures by health plans to employers. We also recognize that employers are paying for health care in many cases, and it has been suggested to us that they may need access to claims and other information for the purposes of negotiating rates, quality improvement and auditing their plans and claims administrators. We invite comment on the extent to which employers currently receive protected health information about their employees, for what types of activities protected health information is received, and whether any or all of these activities could be accomplished with de-identified health information. We also invite other comments on how disclosures to employers should be treated under this rule.

22. *Protected health information.* We would create a new definition of ''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 example, protected health information would remain protected after it is read from a computer screen and discussed orally, printed onto paper or other media, photographed, or otherwise duplicated. We note that individually identifiable health information created or received by an employer as such would not be considered protected health information, although such information created or received by an employer in its role as a health plan or provider would be protected health information.

Under this definition, information that is ''electronically transmitted'' would include information exchanged with a computer using electronic media, even when the information is physically

moved from one location to another using magnetic or optical media (e.g., copying information from one computer to another using a floppy disc). Transmissions over the Internet (i.e., open network), Extranet (i.e., using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, and private networks would all be included. Telephone voice response and ''faxback'' (i.e., a request for information from a computer made via voice or telephone keypad input with the requested information returned as a fax) systems would be included because these are computer output devices similar in function to a printer or video screen. This definition would not include ''paper-to-paper'' faxes, or person-to-person telephone calls, video teleconferencing, or messages left on voice-mail. The key concept that determines if a transmission meets the definition is whether the source or target of the transmission is a computer. The medium or the machine through which the information is transmitted or rendered is irrelevant.

Also, information that is ''electronically maintained'' would be information stored by a computer or on any electronic medium from which the information may be retrieved by a computer. These media include, but are not limited to, electronic memory chips, magnetic tape, magnetic disk, or compact disc (CD) optical media.

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, would not be considered protected health information. Congress specifically addressed such information when it enacted FERPA to protect the privacy rights of students and parents in educational settings. FERPA applies to educational records that are maintained by educational agencies and institutions that are recipients of federal funds from the Department of Education. FERPA requires written consent of the parent or student prior to disclosure of education records except in statutorily specified circumstances. We do not believe that Congress intended to amend or preempt FERPA in enacting HIPAA.

Individually identifiable health information of inmates of correctional facilities and detainees in detention facilities would be excluded from this definition because unimpeded sharing of inmate identifiable health information is crucial for correctional and detention facility operations. In a correctional or detention setting, prison officials are required by law to safely house and provide health care to inmates. These activities require the use and disclosure of identifiable health information. Therefore, correctional and detention facilities must routinely share inmate health information among their health care and other components, as well as with community health care facilities. In order to maintain good order and protect the well-being of prisoners, the relationship between such facilities and inmates or detainees involves a highly regulated, specialized area of the law which has evolved as a carefully balanced compromise with due deference to institutional needs and obligations.

Federal and other prison facilities routinely share health information with community health care facilities in order to provide medical treatment to persons in their custody. It is not uncommon for inmates and detainees to be transported from one facility to another, for example, for the purpose of making a court appearance in another jurisdiction, or to obtain specialized medical care. In these and other circumstances, law enforcement agencies such as the Federal Bureau of Prisons (the Bureau), the United States Marshals Service (USMS), the Immigration and Naturalization Service, State prisons, county jails, and U.S. Probation Offices, share identifiable health information about inmates and detainees to ensure that appropriate health care and supervision of the inmate or detainee is maintained. Likewise, these agencies must, in turn, share health information with the facility that resumes custody of the inmate or detainee.

Requiring an inmate's or detainee's authorization for disclosure of identifiable health information for day-to-day operations would represent a significant shift in correctional and detention management philosophy. If correctional and detention facilities were covered by this rule, the proposed provisions for individual authorizations could potentially be used by an inmate or detainee to override the safety and security concerns of the correctional/custodial authority; for example, an inmate being sent out on a federal writ could refuse to permit the Bureau to disclose a suicide history to the USMS. Additionally, by seeking an authorization to disclose the information, staff may give the inmate or detainee advance notice of an impending transfer, which in turn may create security risks.

Therefore we propose to exclude the individually identifiable health information of inmates of correctional facilities and detainees in detention facilities from the definition of protected health information. We note that existing federal laws limiting the disclosure and release of information (e.g., FOIA/Privacy Act) protect the privacy of identifiable federal inmate health information. Subject to certain limitations, these laws permit inmates and detainees to obtain and review a copy of their medical records and to correct inaccurate information.

Under this approach, the identifiable health information held by correctional and detention facilities of persons who have been released would not be protected. The facilities require continued access to such information for security, protection and health care purposes because inmates and detainees are frequently readmitted to correctional and detention facilities. However, concern has been expressed about the possibility that absent coverage by this proposed rule, correctional and detention facilities may disclose information about former inmates and detainees without restriction. We therefore request comments on whether identifiable health information held by correctional and detention facilities about former inmates and detainees should be subject to this rule, and the potential security concerns and burden such a requirement might place on these facilities.

23. *Psychotherapy notes.* We would define ''psychotherapy notes'' to mean detailed 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. Such notes are used only by the therapist who wrote them, maintained separately from the medical record, and not involved in the documentation necessary for health care treatment, payment, or operations. Such term would not include medication prescription and monitoring, counseling session start and stop times or the modalities and frequencies of treatment furnished, results of clinical tests, or a brief summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis and progress to date.

24. *Public health authority.* We would define ''public health authority'' 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 that is responsible for public health matters as part of its official mandate.

25. *Research.* We would define ''research'' as a systematic investigation,

including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge. We further explain that ''generalizable knowledge'' is knowledge related to health that can be applied to populations outside of the population served by the covered entity.

This is the definition of ''research'' in the federal regulation that protects human subjects, entitled The Federal Policy for the Protection of Human Subjects (often referred to as the ''Common Rule,'' at 45 CFR part 46). This definition is well understood in the research community and elsewhere, and we propose to use it here to maintain consistency with other federal regulations that affect research.

26. *Research information unrelated to treatment.* We would define ''research information unrelated to treatment'' as information that is received or created by a covered entity in the course of conducting research for which there is insufficient scientific and medical evidence regarding the validity or utility of the information such that it should not be used for the purpose of providing health care,[2] and with respect to which the covered entity has not requested payment from a health plan.

27. *Treatment.* We would define ''treatment'' to mean 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, or the referral of an individual from one provider to another, or coordination of health care or other services among health care providers and third parties authorized by the health plan or the individual. Our definition is intended to relate only to services provided to an individual and not to an entire enrolled population.

28. *Use.* We would propose a new definition of the term ''use'' to mean the employment, application, utilization, examination or analysis of health information within an entity that holds the information.

29. *Workforce.* We would 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.

[2] For example, *validity* is an indicator of how well a test measures the property or characteristic it is intended to measure and the reliability of a test, *i.e.*, whether the same result is obtained each time the test is used. Validity is also a measurement of the accuracy with which a test predicts a clinical condition. *Utility* refers to the degree to which the results of test can be used to make decisions about the subsequent delivery of health care.

C. General Rules. (§ 164.506)

[*Please label comments about this section with the subject: ''Introduction to general rules''*]

The purpose of our proposal is to define and limit the circumstances in which an individual's protected health information could be used or disclosed by covered entities. As discussed above, we are proposing to make the use and exchange of protected health information relatively easy for health care purposes and more difficult for purposes other than health care.

As a general rule, we are proposing that protected health information not be used or disclosed by covered entities except as authorized by the individual who is the subject of such information or as explicitly provided by this rule. Under this proposal, most uses and disclosures of an individual's protected health information would not require explicit authorization by the individual, but would be restricted by the provisions of the rule. Covered entities would be able to use or disclose an individual's protected health information without authorization for treatment, payment and health care operations. See proposed § 164.506(a)(1)(i). Covered entities also would be permitted 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. Covered entities would be *permitted* by this rule to use and disclose protected health information when required to do so by other law, such as a mandatory reporting requirement under State law or pursuant to a search warrant. See proposed § 164.510. Covered entities would be *required* by this rule to disclose protected health information for only two purposes: To permit individuals to inspect and copy protected health information about them (see proposed § 164.514) and for enforcement of this rule (see proposed § 164.522(e)).

The proposed rule generally would not require covered entities to vary the level of protection of protected health information based on the sensitivity of such information. We believe that all protected health information should have effective protection from inappropriate use and disclosure by covered entities, and except for limited classes of information that are not needed for treatment and payment purposes, we have not provided additional protection to protected health information that might be considered particularly sensitive. We would note that the proposed rule would not preempt provisions of other applicable laws that provide additional privacy protection to certain classes of protected health information. We understand, however, that there are medical conditions and treatments that individuals may believe are particularly sensitive, or which could be the basis of stigma or discrimination. We invite comment on whether this rule should provide for additional protection for such information. We would appreciate comment that discusses how such information should be identified and the types of steps that covered entities could take to provide such additional protection. We also invite comment on how such provisions could be enforced.

Covered entities of all types and sizes would be required to comply with the proposed privacy standards outlined below. The proposed standards would not impose particular mechanisms or procedures that covered entities must adopt to implement the standards. Instead, we would 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. How each privacy standard would be satisfied would be business decisions that each entity would have to make. This allows the privacy standards to establish a stable baseline, yet remain flexible enough to take advantage of developments and methods for protecting privacy that will evolve over time.

Because the privacy standards would need to be implemented by all covered entities, from the smallest provider to the largest, multi-state health plan, a single approach to implementing these standards would be neither economically feasible nor effective in 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 duties (see proposed § 164.518(a)) whereas at a large health plan, the privacy official may constitute a full time position and have the regular support and advice of a privacy staff or board.

Similarly, a large enterprise may make frequent electronic disclosures of similar data. In such a case, the enterprise would be expected to remove identifiers or to limit the data fields that are disclosed to fit the purpose of the disclosure. The process would be documented and perhaps even automated. A solo physician's office, however, would not be expected to have

the same capabilities to limit the amount of information disclosed, although, in the cases of disclosures involving a small number of records, such an office could be expected to hide identifiers or to limit disclosures to certain pages of the medical record that are relevant to the purpose of the disclosure.

In taking this approach, we intend to strike a balance between the need to maintain the confidentiality of protected health information and the economic cost of doing so. Health care entities must consider both aspects in devising their solutions. This approach is similar to the approach we proposed in the Notice of Proposed Rulemaking for the administrative simplification security and electronic signature standards.

1. Use and Disclosure for Treatment, Payment, and Health Care Operations. (§ 164.506(a))

[*Please label comments about this section with the subject: ''Treatment, payment, and health care operations''*]

We are proposing that, subject to limited exceptions for psychotherapy notes and research information unrelated to treatment discussed below, a covered entity be permitted to use or disclose protected health information without individual authorization for treatment, payment or health care operations.

The Secretary's Recommendations proposed that covered entities be able to use individually identifiable health information without authorization of the identified individual for treatment and payment and for purposes that are ''compatible with and directly related to'' treatment and payment. The Recommendations further explained that the terms ''treatment'' and ''payment'' were to be construed broadly, encompassing treatment and payment for all patients. They also noted that the test of ''compatible with and directly related to'' is meant to be more restrictive than the test currently used in the Privacy Act, 5. U.S.C. 552a, for determining whether a proposed ''routine use'' is sufficiently related to the primary purpose for which the information would be collected to permit its release under the proposed ''routine use.'' The Privacy Act permits release of such information if the proposed routine use is ''compatible with'' the purpose for which the information is collected. Our proposal is intended to be consistent with this discussion from the Secretary's Recommendations.

a. *General rule for treatment, payment, and health care operations.* We are not proposing to require individual authorizations of uses and disclosures for health care and related purposes, although such authorizations are routinely gathered today as a condition of obtaining health care or enrolling in a health plan. Although many current disclosures of health information are made pursuant to individual authorizations, these authorizations provide individuals with little actual control over their health information. When an individual is required to sign a blanket authorization at the point of receiving care or enrolling for coverage, that consent is often not voluntary because the individual must sign the form as a condition of treatment or payment for treatment. Individuals are also often asked to sign broad authorizations but are provided little or no information about how their health information may be or will in fact be used. Individuals cannot make a truly informed decision without knowing all the possible uses, disclosures and re-disclosures to which their information will be subject. In addition, since the authorization usually precedes creation of the record, the individual cannot predict all the information the record may contain and therefore cannot make an informed decision as to what would be released.

Our proposal is intended to make the exchange of protected health information relatively easy for health care purposes and more difficult for purposes other than health care. For individuals, health care treatment and payment are the core functions of the health care system. This is what they expect their health information will be used for when they seek medical care and present their proof of insurance to the provider. Consistent with this expectation, we considered requiring a separate individual authorization for every use or disclosure of information but rejected such an approach because it would not be realistic in an increasingly integrated health care system. For example, a requirement for separate patient authorization for each routine referral could impair care, by delaying consultation and referral, as well as payment.

We therefore propose that covered entities be permitted to use and disclose protected health information without individual authorization for treatment and payment purposes, and for related purposes that we have defined as health care operations. For example, health care providers could maintain and refer to a medical record, disclose information to other providers or persons as necessary for consultation about diagnosis or treatment, and disclose information as part of referrals to other providers. Health care providers also could use a patient's protected health information for payment purposes such as submitting a claim to a payer. In addition, they could use a patient's protected health information for health care operations, such as use for an internal quality oversight review. We would note that, in the case of an individual where the provider has agreed to restrictions on use or disclosure of the patient's protected health information, the provider is bound by such restrictions as provided in § 164.506(c).

Similarly, health plans could use an enrollee's protected health information for payment purposes, such as reviewing and paying health claims that have been submitted to it, pre-admission screening of a request for hospitalization, or post-claim audits of health care providers. Health plans also could use an enrollee's protected health information for health care operations, such as reviewing the utilization patterns or outcome performance of providers participating in their network.

Further, as described in more detail below, health care providers and health plans would not need individual authorization to provide protected health information to a business partner for treatment, payment or health care operations functions if the other requirements for disclosing to business partners are met. See proposed § 164.506(e).

We intend that the right to use and disclose protected health information be interpreted to apply for treatment and payment of all individuals. For example, in the course of providing care to a patient, a physician could wish to examine the records of other patients with similar conditions. Likewise, a physician could consult the records of several people in the same family or living in the same household to assist in diagnosis of conditions that could be contagious or that could arise from a common environmental factor. A health plan or a provider could use the protected health information of a number of enrollees to develop treatment protocols, practice guidelines, or to assess quality of care. All of these uses would be permitted under this proposed rule.

Our proposal would not restrict to whom disclosures could be made for treatment, payment or operations. For example, covered entities could make disclosures to non-covered entities for payment purposes, such as a disclosure to a workers compensation carrier for coordination of benefits purposes. We note, however, that when disclosures are made to non-covered entities, the

ability of this proposed rule to protect the confidentiality of the information ends. This points to the need for passage of more comprehensive privacy legislation that would permit the restrictions on use and disclosure to follow the information beyond covered entities.

We also propose 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. As discussed above in this section, such authorizations could not provide meaningful privacy protections or individual control and could in fact cultivate in individuals erroneous understandings of their rights and protections.

The general approach that we are proposing is not new. Some existing State health confidentiality laws permit disclosures without individual authorization to other health care providers treating the individual, and the Uniform Health-Care Information Act permits disclosure ''to a person who is providing health-care to the patient'' (9 part I, U.L.A. 475, 2–104 (1988 and Supp. 1998)). We believe that this approach would be the most realistic way to protect individual confidentiality in an increasingly data-driven, electronic and integrated health care system. We recognize, however, that particularly given the limited scope of the authority that we have under this proposed rule to reach some significant actors in the health care system, that other approaches could be of interest. We invite comments on whether other approaches to protecting individuals' health information would be more effective.

b. *Health care operations.* We considered the extent to which the covered entities might benefit from further guidance on the types of activities that appropriately would be considered health care operations. The term is defined in proposed § 164.504. In the debates that have surrounded privacy legislation before the Congress, there has been substantial discussion of the definition of health care operations, with some parties advocating for a very broad definition and others advocating a more restrictive approach.

Given the lack of consensus over the extent of the activities that could be encompassed within the term health care operations, we determined that it would be helpful to identify activities that, in our opinion, are sufficiently unrelated to the treatment and payment functions to require a individual to authorize use of his or her information. We want to make clear that these activities would not be prohibited, and do not dispute that many of these activities are indeed beneficial to both individuals and the institutions involved. Nonetheless, they are not necessary for the key functions of treatment and payment and therefore would require the authorization of the individual before his/her information could be used. These activities would include but would not be limited to:

- The use of protected health information for marketing of health and non-health items and services;
- The disclosure of protected health information for sale, rent or barter;
- The use of protected health information by a non-health related division of the same corporation, e.g., for use in marketing or underwriting life or casualty insurance, or in banking services;
- The disclosure, by sale or otherwise, of protected health information to a plan or provider for making eligibility or enrollment determinations, or for underwriting or risk rating determinations, prior to the individual's enrollment in the plan;
- The disclosure of information to an employer for use in employment determinations; and
- The use or disclosure of information for fund raising purposes.

We invite comments on the activities within the proposed definitions of ''treatment,'' ''payment,'' and ''health care operations,'' as well as the activities proposed to be excluded from these definitions.

c. *Exception for psychotherapy notes.* We propose that a covered health care provider not be permitted to disclose psychotherapy notes, as defined by this proposed rule, for treatment, payment, or health care operations unless a specific authorization is obtained from the individual. In addition, a covered entity would not be permitted to condition treatment of an individual, enrollment of an individual in a health plan, or payment of a claim for benefits made by or on behalf of an individual on a requirement that the individual provide a specific authorization for the disclosure of psychotherapy notes.

We would define ''psychotherapy notes'' to mean detailed 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. Such notes could be used only by the therapist who wrote them, would have to be maintained separately from the medical record, and could not be involved in the documentation necessary for health care treatment, payment, or operations (as defined in § 164.504). Such term would not include medication prescription and monitoring, counseling session start and stop times or the modalities and frequencies of treatment furnished, results of clinical tests, or summaries of the following items: diagnoses, functional status, the treatment plan, symptoms, prognosis and progress to date.

Psychotherapy notes are of primary value to the specific provider and the promise of strict confidentiality helps to ensure that the patient will feel comfortable freely and completely disclosing very personal information essential to successful treatment. Unlike information shared with other health care providers for the purposes of treatment, psychotherapy notes are more detailed and subjective and are subject to unique rules of disclosure. In *Jaffee* v. *Redmond,* 518 U. S. 1 (1996), the Supreme Court ruled that conversations and notes between a patient and psychotherapist are confidential and protected from compulsory disclosure. The language in the Supreme Court opinion makes the rationale clear:

> Like the spousal and attorney-client privileges, the psychotherapist-patient privilege is ''rooted in the imperative need for confidence and trust.'' * * * Treatment by a physician for physical ailments can often proceed successfully on the basis of a physical examination, objective information supplied by the patient, and the results of diagnostic tests. Effective psychotherapy, by contrast, depends upon an atmosphere of confidence and trust in which the patient is willing to make a frank and complete disclosure of facts, emotions, memories, and fears. Because of the sensitive nature of the problems for which individuals consult psychotherapists, disclosure of confidential communications made during counseling sessions may cause embarrassment or disgrace. For this reason, the mere possibility of disclosure may impede development of the confidential relationship necessary for successful treatment. As the Judicial Conference Advisory Committee observed in 1972 when it recommended that Congress recognize a psychotherapist privilege as part of the Proposed Federal Rules of Evidence, a psychiatrist's ability to help her patients ''is completely dependent upon (the patients') willingness and ability to talk freely. This makes it difficult if not impossible for (a psychiatrist) to function without being able to assure * * * patients of confidentiality and, indeed, privileged communication. Where there may be exceptions to this general rule * * *, there is wide agreement that confidentiality is a *sine qua non* for successful psychiatric treatment. * * *''

By protecting confidential communications between a psychotherapist and her patient

from involuntary disclosure, the proposed privilege thus serves important private interests. * * * The psychotherapist privilege serves the public interest by facilitating the provision of 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.

That it is appropriate for the federal courts to recognize a psychotherapist privilege under Rule 501 is confirmed by the fact that all 50 States and the District of Columbia have enacted into law some form of psychotherapist privilege. * * * Because state legislatures are fully aware of the need to protect the integrity of the fact finding functions of their courts, the existence of a consensus among the States indicates that ''reason and experience'' support recognition of the privilege. In addition, given the importance of the patient's understanding that her communications with her therapist will not be publicly disclosed, any State's promise of confidentiality would have little value if the patient were aware that the privilege would not be honored in a federal court. * * * *Jaffee,* 518 U.S. 7–9.

The special status of the psychotherapist privilege in our society as well as the physical and conceptual segregation of the psychotherapy notes makes this prohibition on disclosures for treatment, payment and health care operations without a specific authorization from the individual reasonable and practical.

We note that the policy being applied to psychotherapy notes differs from the policy being applied to most other types of protected health information. For most protected health information, a covered entity would be prohibited from soliciting an authorization from an individual for treatment, payment and health operations unless such an authorization is required by other applicable law. In this case, because of the special status of psychotherapy notes as described above, we propose that a specific authorization be required before such notes can be disclosed within the treatment and payment systems. We propose this special treatment because there are few reasons why other health care entities should need the psychotherapy notes about an individual, and in those cases, the individual is in the best position to determine if the notes should be disclosed. For example, an individual could authorize disclosure if they are changing health care providers. Since we have defined psychotherapy notes in such a way that they do not include information that health plans would need to process a claim for services, special authorizations for payment purposes should be rare. We would note that the provisions governing authorizations under § 164.508 would apply to the special authorizations under this provision.

We also propose that covered entities not be permitted to condition treatment or payment decisions on a requirement that an individual provide a specific authorization for the use or disclosure of psychotherapy notes. The special protections that are being proposed would not be meaningful if covered entities could coerce individuals by conditioning treatment or payment decisions on a requirement that the individual authorize use or disclosures of such notes. This requirement would not prohibit the provider that creates the psychotherapy notes information from using the notes for treatment of the individual. The provider could not, however, condition the provision of treatment on a requirement that the individual authorize the use of the psychotherapy notes by the covered entity for other purposes or the disclosure of the notes by the provider to others.

We considered including other disclosures permitted under proposed § 164.510 within the prohibition described in this provision, but were unsure if psychotherapy notes were ever relevant to the public policy purposes underlying those disclosures. For example, we would assume that such notes are rarely disclosed for public health purposes or to next of kin. We solicit comment on whether there are additional categories of disclosures permitted under proposed § 164.510 for which the disclosure of psychotherapy notes by covered entities without specific individual authorization would be appropriate.

d. *Exception for research information unrelated to treatment.* Given the voluntary, often altruistic, nature of research participation, and the experimental character of data generated from many research studies, research participants should have assurances that the confidentiality of their individually identifiable information will be maintained in a manner that respects these unique characteristics. In the process of conducting health research, some information that is collected could be related to the delivery of health care to the individual and some could be unrelated to the care of the individual. Some information that is generated in the course of a research study could have unknown analytic validity, clinical validity, or clinical utility. In general, unknown analytic or clinical validity means that the sensitivity, specificity, and predictive value of the research information is not known. Specifically, analytic validity refers to how well a test performs in measuring the property or characteristic it is intended to measure. Another element of the test's analytical validity is its reliability—that is, it must give the same result each time. Clinical validity is the accuracy with which a test predicts a clinical condition. Unknown clinical utility means that there is an absence of scientific and medical agreement regarding the applicability of the information for the diagnosis, prevention, or treatment of any malady, or the assessment of the health of the individual.

We would define ''research information unrelated to treatment'' as information that is received or created by a covered entity in the course of conducting research for which there is insufficient scientific and medical evidence regarding the validity or utility of the information such that it should not be used for the purpose of providing health care, and with respect to which the covered entity has not requested payment from a health plan.

Such information should never be used in a clinical treatment protocol but could result as a byproduct of such a protocol. For example, consider a study which involves the evaluation of a new drug, as well as an assessment of a genetic marker. The drug trial includes physical and radiographic examinations, as well as blood tests to monitor potential toxicity of the new drug on the liver; all of these procedures are part of the provision of health care, and therefore, would constitute ''protected health information,'' but not ''research information unrelated to treatment.'' In the same study, the investigators are searching for a genetic marker for this particular disease. To date, no marker has been identified and it is uncertain whether or not the preliminary results from this research study would prove to be a marker for this disease. The genetic information generated from this study would constitute ''research information unrelated to treatment''.

We solicit comment on this definition of ''research information unrelated to treatment'' and how it would work in practice.

Because the meaning of this information is currently unknown, we would prohibit its use and disclosure for treatment, payment and health care operations unless a specific authorization is obtained from the subject of the information. Failing to limit the uses and disclosures of this information within the health payment system would place research participants at increased risk of discrimination, which could result in

individuals refusing to volunteer to participate in this type of research. Without the special protections that we are proposing, we are concerned that much potentially life-saving research could be halted. Moreover, because this information that lacks analytical or clinical validity and clinical utility, and because we have defined it in terms that preclude researchers from seeking third-party reimbursement for its creation, there would not be a reason for this information to be further used or disclosed within the treatment and payment system without individual authorization.

We also propose that covered entities not be permitted to condition treatment or payment decisions on a requirement that an individual provide a specific authorization for the use or disclosure of research information unrelated to treatment. The special protections that are being proposed would not be meaningful if covered entities could coerce individuals into authorizing disclosure by conditioning treatment or payment decisions on a requirement that the individual authorize disclosures of such information. This requirement would not prohibit the covered entity that creates the information from using the information for the research purposes for which it was collected. The entity could not, however, condition the provision of treatment on a requirement that the individual authorize use of research information unrelated to treatment by the covered entity for other purposes or the disclosure of the information by the covered entity to others.

We considered including other of the uses and disclosures that would be permitted under § 164.510 within the prohibition described in this provision, but were unsure if research information unrelated to treatment would ever be relevant to the public policy purposes underlying those disclosures. We solicit comment on whether there are additional categories of uses or disclosures that would be permitted under proposed § 164.510 for which the use or disclosure of such information by covered entities without specific individual authorization would be appropriate.

2. Minimum Necessary Use and Disclosure. (§ 164.506(b))

[*Please label comments about this section with the subject: ''Minimum necessary''*]

We propose that, except as discussed below, a covered entity must 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, taking into consideration practical and technological limitations.

In certain circumstances, the assessment of what is minimally necessary is appropriately made by a person other than the covered entity; in those cases, discussed in this paragraph, and reflected in proposed § 164.506(b)(1)(i), the requirements of this section would not apply. First, the covered entity would not be required to make a ''minimum necessary'' analysis for the standardized content of the various HIPAA transactions, since that content has been determined through regulation. Second, with one exception, when an individual authorizes a use or disclosure the covered entity would not be required to make a ''minimum necessary'' determination. In such cases, the covered entity would be unlikely to know enough about the information needs of the third party to make a ''minimum necessary'' determination. The exception, when the ''minimum necessary'' principle would apply to an authorization, is for authorizations for use of protected health information by the covered entity itself. See proposed § 164.508(a)(2). Third, with respect to disclosures that are mandatory under this or other law, and which would be permitted under the rules proposed below, public officials, rather than the covered entity, would determine what information is required (e.g., coroners and medical examiners, State reporting requirements, judicial warrants). See proposed §§ 164.510 and 164.506(b)(1)(ii). Fourth, disclosure made pursuant to a request by the individual for access to his or her protected health information presents no possible privacy threat and therefore lies outside this requirement. See proposed § 164.506(b)(1)(i).

Under this proposal, covered entities generally would be required to establish policies and procedures to limit the amount of protected health care information used or disclosed to the minimum amount necessary to meet the purpose of the use or disclosure, and to limit access to protected health information only to those people who need access to the information to accomplish the use or disclosure. With respect to use, if an entity consists of several different components, the entity would be required to create barriers between components so that information is not used inappropriately. For example, a health plan that offers other insurance products would have policies and procedures to prevent protected health information from crossing over from one product line to another. The same principle applies to disclosures. For example, if a covered entity opts to disclose protected health information to a researcher pursuant to proposed § 164.510(j), it would need to ensure that only the information necessary for the particular research protocol is disclosed.

It should be noted that, under section 1173(d) of the Act, covered entities would also be required to satisfy the requirements of the Security standards, by establishing policies and procedures to provide access to health information systems only to persons who require access, and implement procedures to eliminate all other access. Thus, the privacy and security requirements would work together to minimize the amount of information shared, thereby lessening the possibility of misuse or inadvertent release.

A ''minimum necessary'' determination would need to be consistent with and directly related to the purpose of the use or disclosure and take into consideration the ability of a covered entity to delimit the amount of information used or disclosed and the relative burden imposed on the entity. The proposed minimum necessary requirement is based on a reasonableness standard: covered entities would be required to make reasonable efforts and to incur reasonable expense to limit the use and disclosure of protected health information as provided in this section.

In determining what a reasonable effort is under this section, covered entities should take into consideration the amount of information that would be used or disclosed, the extent to which the use or disclosure would extend the number of individuals or entities with access to the protected health information, the importance of the use or disclosure, the likelihood that further uses or disclosures of the protected health information could occur, the potential to achieve substantially the same purpose with de-identified information, the technology available to limit the amount of protected health information that is used or disclosed, the cost of limiting the use or disclosure, and any other factors that the covered entity believes are relevant to the determination. We would expect that in most cases where covered entities have more information than is necessary to accomplish the purpose of a use or disclosure, some method of limiting the information that is used or disclosed could be found.

We note that all of the uses and disclosures subject to the requirements of this provision are permissive; the minimum necessary provision does not

apply to uses or disclosures mandated by law. Covered entities should not make uses or disclosures of protected health information where they are unable to make any efforts to reasonably limit the amount of protected health information used or disclosed for a permissive purpose. Where there is ambiguity regarding the particular information to be used or disclosed, this provision should be interpreted to require the covered entity or make some effort to limit the amount of information used or disclosed.

We note that procedures for implementing the minimum necessary requirement for uses would often focus on limiting the physical access that employees, business partners and others would have to the protected health information. Procedures which limit the specific employees or business partners, or the types of employees or business partners, who would be qualified to gain access to particular records would often be appropriate. Covered entities with advanced technological capabilities should also consider limiting access to appropriate portions of protected health information when it would be practical to do so.

The ''minimum necessary'' determination would include a determination that the purpose of the use or disclosure could not be reasonably accomplished with information that is not identifiable. Each covered entity would be required to have policies for determining when information must be stripped of identifiers before disclosure. If identifiers are not removed simply because of inconvenience to the covered entity, the ''minimum necessary'' rule would be violated.

Similarly, 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'' rule. Except where the individual has specifically authorized use or disclosure of the full medical record, when a covered entity receives a request for an entire medical record, the covered entity could not, under these proposed rules, disclose the entire record unless the request included an explanation of why the purpose of the disclosure could not reasonably be accomplished without the entire medical record.

The decisions called for in determining what would be the minimum necessary information to accomplish an allowable purpose should include both a respect for the privacy rights of the subjects of the medical record and the reasonable ability of covered entities to delimit the amount of individually identifiable health information in otherwise permitted uses and disclosures. For example, a large enterprise that makes frequent electronic disclosures of similar data would be expected to remove identifiers or to limit the data fields that are disclosed to fit the purpose of the disclosure. An individual physician's office would not be expected to have the same capabilities to limit the amount of information disclosed, although, in the cases of disclosures involving a small number of records, such an office could be expected to hide identifiers or to limit disclosures to certain pages of the medical record that are relevant to the purpose of the disclosure.

Even where it might not be reasonable for a covered entity to limit the amount of information disclosed, there could be opportunities, when the use or disclosure does not require authorization by the individual, to reduce the scope of the disclosure in ways that substantially protect the privacy interests of the subject. For example, if a health researcher wants access to relatively discrete parts of medical records that are presently maintained in paper form for a large number of patients with a certain condition, it could be financially prohibitive for the covered entity to isolate the desired information. However, it could be reasonable for the covered entity to allow the researcher to review the records on-site and to abstract only the information relevant to the research. Much records research is done today through such abstracting, and this could be a good way to meet the ''minimum necessary'' principle. By limiting the physical distribution of the record, the covered entity would have effectively limited the scope of the disclosure to the information necessary for the purpose.

Proposed § 164.506(b) generally would place the responsibility for determining what disclosure is the ''minimum necessary'' on the covered entity making the disclosure. The exception would be for health plan requests for information from health care providers for auditing and related purposes. In this instance, since the provider is not in a position to negotiate with the payer, the duty would be shifted to the payer to request the ''minimum necessary'' information for the purpose. See proposed § 164.506(b)(1)(iv). Whenever a health plan requests a disclosure, it would be required to limit its requests to the information to achieve the purpose of the request. For example, a health plan seeking protected health information from a provider or other health plan to process a payment should not request the entire health record unless it is actually necessary.

In addition, the proposal would permit covered entities to reasonably rely on requests by certain public agencies in determining the minimum necessary information for certain disclosures. For example, a covered entity that reasonably relies on the requests of public health agencies, oversight agencies, law enforcement agencies, coroners or medical examiners would be in compliance with this requirement. See proposed § 164.506(b)(3).

As discussed in prior HIPAA proposed rulemakings, it is likely to be easier to limit disclosure when disclosing computerized records than when providing access to paper records. Technological mechanisms to limit the amount of information available for a particular purpose, and make information available without identifiers, are an important contribution of technology to personal privacy. For example, the fields of information that are disclosed can be limited, identifiers (including names, addresses and other data) can be removed, and encryption can restrict to authorized personnel the ability to link identifiers back to the record.

For electronic information covered by the proposed rules, the ''minimum necessary'' requirement would mean reviewing, forwarding, or printing out only those fields and records relevant to the user's need for information. Where reasonable (based on the size, sophistication and volume of the covered entity's electronic information systems), covered entities would configure their record systems to allow selective access to different portions of the record, so that, for example, administrative personnel get access to only certain fields, and medical personnel get access to other fields. This selective access to information would be implemented using the access control technology discussed in the electronic security regulation.

For non-electronic information covered by the proposed rules, ''minimum necessary'' would mean the selective copying of relevant parts of protected health information or the use of ''order forms'' to convey the relevant information. These techniques are already in use in the health care environment today, not because of privacy considerations, but because of the risk of losing access to the full medical record when needed for clinic or emergency visits.

This rule would require, in proposed § 164.520, that each covered entity document the administrative policies and procedures that it will use to meet the requirements of this section. With respect to the ''minimum necessary'' compliance standard, such procedures would have to describe the process or processes by which the covered entity will make minimum necessary determinations, the person or persons who will be responsible for making such determinations, and the process in place to periodically review routine uses and disclosures in light of new technologies or other relevant changes. Proposed uses or disclosures would have to be reviewed by persons who have an understanding of the entity's privacy policies and practices, and who have sufficient expertise to understand and weigh the factors described above. See proposed § 164.506(b)(2). The policies that would be reasonable would vary depending on the nature and size of the covered entity. For large enterprises, the documentation of policies and procedures might identify the general job descriptions of the people that would make such decisions throughout the organization.

In addition, the procedures would provide that the covered entity will review each request for disclosure individually on its own merits (and, for research, the documentation of required IRB or other approval). Covered entities should not have general policies of approving all requests (or all requests of a particular type) for disclosures or uses without carefully considering the factors identified above as well as other information specific to the request that the entity finds important to the decision.

We understand that the requirements outlined in this section do not create a bright line test for determining the minimum necessary amount of protected health information appropriate for most uses or disclosures. Because of this lack of precision, we considered eliminating the requirement altogether. We also considered merely requiring covered entities to address the concept within their internal privacy procedures, with no further guidance as to how each covered entity would address the issue. These approaches were rejected because minimizing both the amount of protected health information used and disclosed within the health care system and the number of persons who have access to such information is vital if we are to successfully enhance the confidentiality of people's personal health information. We invite comments on the approach that we have adopted and on alternative methods of implementing the minimum necessary principle.

3. Right to Restrict Uses and Disclosures. (§ 164.506(c))

[*Please label comments about this section with the subject: ''Right to restrict''*]

We propose to permit in § 164.506(c) that individuals be able to request that a covered entity restrict further uses and disclosures of protected health information for treatment, payment, or health care operations, and if the covered entity agrees to the requested restrictions, the covered entity could not make uses or disclosures for treatment, payment or health care operations that are inconsistent with such restrictions, unless such uses or disclosures are mandated by law. This provision would not apply to health care provided to an individual on an emergency basis.

This proposal would not restrict the right of a provider to make an otherwise permissible disclosure under § 164.510, such as a disclosure for public health or emergency purposes. While there is nothing in this proposed rule that would prohibit a provider and an individual from agreeing in advance not to make such disclosures, such an agreement would not be enforceable through this proposed rule.

We should note that there is nothing in this proposed rule that requires a covered entity to agree to a request to restrict, or to treat or provide coverage to an individual requesting a restriction under this provision. Covered entities who do not wish to, or due to contractual obligations cannot, restrict further use or disclosure would not be obligated to treat an individual making a request under this provision. For example, some health care providers could feel that it is medically inappropriate to honor patient requests under this provision. The medical history and records of a patient, particularly information about current medications and other therapies, are often very much relevant when new treatment is sought, and the patient cannot seek to withhold this information from subsequent providers without risk.

Under this proposal, individuals could request broad restrictions on further uses and disclosures for treatment, payment or health care operations, or could request more limited restrictions relating to further uses or disclosures of particular portions of the protected health information or to further disclosures to particular persons. Covered entities could choose to honor the individual's request, could decline to treat or provide coverage to the individual, or could propose an alternative restriction of further use or disclosure. The covered entity would not be bound by an individual's request for restriction until its scope has been agreed to by the individual and the provider. Once an agreement has been reached, however, a covered entity that uses or discloses the protected health information resulting from the encounter in any manner that violates such agreement would be in violation of this provision.

We are not proposing to extend this right to individuals receiving emergency medical care, because emergency situations may not afford sufficient opportunity for the provider and patient to discuss the potential implications of restricting further use and disclosure of the resulting medical information. Additionally, a health care provider may not be free to refuse treatment to an emergency patient if the provider does not wish to honor a request to restrict further use or disclosure of health information, leaving the provider in an unfair position where she or he must choose between permitting medical harm to come to the patient or honoring a request that she or he feels may be inappropriate or which may violate the provider's business practices or contractual obligations. Some health care providers are legally required to treat emergency patients (e.g., hospital emergency rooms), and would have no opportunity to refuse treatment as a result of a request to restrict further use and disclosure under this provision. Under the pressure of an emergency, a provider should not be expected to adhere to the restrictions associated with a particular individual's information.

Under this proposal, covered entities would not be responsible for ensuring that agreed-upon restrictions are honored when the protected health information leaves the control of the covered entity or its business partners. For example, a provider would not be out of compliance if information she or he disclosed to another provider (consistent with the agreed upon restrictions and with notice of the applicable restrictions on uses and disclosures) is subsequently used or disclosed in violation of the restrictions.

The agreement to restrict use and disclosure under this provision would have to be documented to be binding on the covered entity. In proposed § 164.520, we would require covered entities to develop and document policies and procedures reasonably designed to ensure that the requests are followed, i.e., that unauthorized uses and disclosures are not made.

We note that this proposed rule would not permit covered entities to require individuals to invoke their right to restrict uses and disclosures; only the patient could make a request and invoke this right to restrict.

We considered providing individuals substantially more control over their protected health information by requiring all covered entities to attempt to accommodate any restrictions on use and disclosure requested by patients. We rejected this option as unworkable. While industry groups have developed principles for requiring patient authorizations, we have not found widely accepted standards for implementing patient restrictions on uses or disclosures. Restrictions on information use or disclosure contained in patient consent forms are sometimes ignored because they may not be read or are lost in files. Thus, it seems unlikely that a requested restriction could successfully follow a patient's information through the health care system—from treatment to payment, through numerous operations, and potentially through certain permissible disclosures. Instead we would limit the provision to restrictions that have been agreed to by the covered entity.

We recognize that the approach that we are proposing could be difficult because of the systems limitations described above. However, we believe that the limited right for patients included in this proposed rule can be implemented because it only applies in instances in which the covered entity agrees to the restrictions. We assume that covered entities would not agree to restrictions that they are unable to implement.

We considered limiting the rights under this provision to patients who pay for their own health care (or for whom no payment was made by a health plan). Individuals and health care providers that engage in self-pay transactions have minimal effect on the rights or responsibilities of payers or other providers, and so there would be few instances when a restriction agreed to in such a situation would have negative implications for the interests of other health care actors. Limiting the right to restrict to self-pay patients also would reduce the number of requests that would be made under this provision. We rejected this approach however, because the desire to restrict further uses and disclosures arises in many instances other than self-pay situations. For example, a patient could request that his or her records not be shared with a particular physician because that physician is a family friend. Or an individual could be seeking a second opinion and might not want his or her treating physician consulted. Individuals have a legitimate interest in restricting disclosures in these situations. We solicit comment on the appropriateness of limiting this provision to instances in which no health plan payment is made on behalf of the individual.

In making this proposal, we recognize that it could be difficult in some instances for patients to have a real opportunity to make agreements with covered entities, because it would not be clear in all cases which representatives of a covered entity could make an agreement on behalf of the covered entity. There also are concerns about the extent to which covered entities could ensure that agreed-upon restrictions would be followed. As mentioned above, current restrictions contained in patient consent forms are sometimes ignored because the person handling the information is unaware of the restrictions. We solicit comments on the administrative burdens this provision creates for covered entities, such as the burdens of administering a system in which some information is protected by federal law and other information is not.

We would note that we expect that systems for handling patient requests to restrict use and disclosure of information will become more responsive as technology develops. Therefore, we will revisit this provision as what is practicable changes over time. Proposed requirements for documenting internal procedures to implement this proposed provision are included in proposed § 164.520. We request comments on whether the final rule should provide examples of appropriate, scalable systems that would be in compliance with this standard.

4. Creation of De-identified Information (164.506(d))

[*Please label comments about this section with the subject: ''Creation of de-identified information''*]

In this rule we are proposing that covered entities and their business partners be permitted to use protected health information to create de-identified health information. Covered entities would be permitted to further use and disclose such de-identified information in any way, provided that they do not disclose the key or other mechanism that would enable the information to be re-identified, and provided that they reasonably believe that such use or disclosure of de-identified information will not result in the use or disclosure of protected health information. See proposed § 164.506(d)(1). This means that a covered entity could not disclose de-identified information to a person if the covered entity reasonably believes that the person would be able to re-identify some or all of that information, unless disclosure of protected health information to such person would be permitted under this proposed rule. In addition, a covered entity could not use or disclose the key to coded identifiers if this rule would not permit the use or disclosure of the identified information to which the key pertains. If a covered entity re-identifies the de-identified information, it may only use or disclose the re-identified information consistent with these proposed rules, as if it were the original protected health information.

In some instances, covered entities creating de-identified health information could want to use codes or identifiers to permit data attributable to the same person to be accumulated over time or across different sources of data. For example, a covered entity could automatically code all billing information as it enters the system, substituting personal identifiers with anonymous codes that permit tracking and matching of data but do not permit people handling the data to create protected health information. Such a mechanism would be permissible as long as the key to unlocking the codes is not available to the people working with the de-identified information, and the entity otherwise makes no attempt to create protected health information from the de-identified information.

There are many instances in which such individually identifiable health information is stripped of the information that could identify individual subjects and is used for analytical, statistical and other related purposes. Large data sets of de-identified information can be used for innumerable purposes that are vital to improving the efficiency and effectiveness of health care delivery, such as epidemiological studies, comparisons of cost, quality or specific outcomes across providers or payers, studies of incidence or prevalence of disease across populations, areas or time, and studies of access to care or differing use patterns across populations, areas or time. Researchers and others often obtain large data sets with de-identified information from providers and payers (including from public payers) to engage in these types of studies. This information is valuable for public health activities (e.g., to identify cost-effective interventions for a particular disease) as well as for

commercial purposes (e.g., to identify areas for marketing new health care services).

We intend that this proposed provision will permit the important health care research that is being conducted today to continue under this rule. Indeed, it would be our 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 research purpose. Such practice would reduce the confidentiality concerns that result from the use of individually identifiable health information for some of these purposes. The selective transfer of health information without identifiers into an analytic database would significantly reduce the potential for privacy violations while allowing broader access to information for analytic purposes, without the overhead of audit trails and IRB review. For example, providing de-identified information to a pharmaceutical manufacturer to use in determining patterns of use of a particular pharmaceutical by general geographic location would be appropriate, even if the information were sold to the manufacturer. Such analysis using protected health information would be research and therefore would require individual authorization or approval by an IRB or similar board. We note that data that includes an individual's address is ''identifiable'' by definition and could not be used in such databases.

We invite comment on the approach that we are proposing and on whether alternative approaches to standards for entities determining when health information can reasonably be considered no longer individually identifiable.

5. Application to business partners. (§ 164.506(e))

[*Please label comments about this section with the subject: ''Business partners''*]

In § 164.506(e), we propose to require covered entities to take specific steps to ensure that protected health information disclosed to a business partner remains protected. We intend these provisions to allow customary business relationships in the health care industry to continue while providing privacy protections to the information shared in these relationships. Business partners would not be permitted to use or disclose protected health information in ways that would not be permitted of the covered entity itself under these rules.

Other than for purposes of consultation or referral for treatment, we would allow covered entities to disclose protected health information to business partners 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 would hold the covered entity responsible for certain violations of this proposed rule made by their business partners, and require assignment of responsibilities when a covered entity acts as a business partner of another covered entity.

a. *Who is a business partner?* Under this proposed rule, a business partner would be 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. This would include 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. This would not include persons who would be members of the covered entity's workforce. The key features of the relationship would be that the business partner is performing an activity or function for or on behalf of the covered entity and that the business partner receives protected health information from the covered entity as part of providing such activity or function.

Many critical functions are performed every day by individuals and organizations that we would define as business partners. Under the proposal, billing agents, auditors, third-party administrators, attorneys, private accreditation organizations, clearinghouses, accountants, data warehouses, consultants and many other actors would be considered business partners of a covered entity. Most covered entities will use one or more business partners, to assist with functions such as claims filing, claims administration, utilization review, data storage, or analysis. For example, if a covered entity seeks accreditation from a private accreditation organization and provides such organization with protected health information as part of the accreditation process, the private accreditation organization would be a business partner of the covered entity. This would be true even if a third party, such as an employer or a public agency, required accreditation as a condition of doing business with it. The accreditation is being performed for the covered entity, not the third party, in such cases.

The covered entity may have business relationships with organizations that would not be considered to be business partners because protected health information is not shared or because services are not provided to the covered entity. For example, a covered entity could contract with another organization for facility management or food services; if these organizations do not receive protected health information for these functions or activities, they would not be considered business partners. In the case where a covered entity provides management services to another organization, the other organization would not be a business partner because it would be receiving, not providing, a service or function.

Under the proposal, a covered entity could become a business partner of another covered entity, such as when a health plan acts as a third-party administrator to an insurance arrangement or a self-funded employee benefit plan. In such cases, we propose that the authority of the covered entity acting as a business partner to use and disclose protected health information be constrained to the authority that any business partner in the same situation would have. Thus, the authority of a covered entity acting as a business partner to use and disclose protected health information obtained as a business partner would be limited by the contract or arrangement that created the business partner relationship.

In most cases, health care clearinghouses would fall under our definition of ''business partner'' because they receive protected health information in order to provide payment processing and other services to health plans, health care providers and their business partners, a case that would fall under our definition of ''business partner.'' Therefore, although health care clearinghouses would be covered entities, in many instances under this proposed rule they would also be treated as business partners of the health care providers or health plans for whom they are performing a service. We would note that because health care clearinghouses would generally be operating as business partners, we are proposing not to apply several requirements to health care clearinghouses that we otherwise would apply to covered plans and providers, such as requiring a notice of information

practices, access for inspection and copying, and accommodation of requests for amendment or correction. See proposed §§ 164.512, 164.514 and 164.516.

b. *Limitations on use or disclosure.*

i. *Scope of the covered entity's authority.*

Under this proposed rule, a business partner would be acting on behalf of a covered entity, and we propose that its use or disclosure of protected health information be limited to the same extent that the covered entity for whom they are acting would be limited. Thus, a business partner could have no more authority to use or disclose protected health information than that possessed by the covered entity from which the business partner received the information. For example, a business partner could not sell protected health information to a financial services firm without individual authorization because the covered entity would not be permitted to do so under these proposed rules. We would note that a business partner's authority to use and disclose protected health information could be further restricted by its contract with a covered entity, as described below.

We are not proposing to require the business partners of covered entities to develop and distribute a notice of information practices, as provided in proposed § 164.512. A business partner would, however, be bound by the terms of the notice of the covered entity from which it obtains protected health information. For example, if a covered entity provided notice to its subscribers that it would not engage in certain permissible disclosures of protected health information, we are proposing that such a limitation would apply to all of the business partners of the covered entity that made the commitment. See proposed § 164.506(e). We are proposing this approach so that individuals could rely on the notices that they receive from the covered entities to which they disclose protected health information. If the business partners of a covered entity were able to make wider use or make more disclosures than the covered entity, the patients or enrollees of the covered entity would have difficulty knowing how their information was being used and to whom it was being disclosed.

ii. *Scope of the contractual agreement.*

We are also proposing that a business partner's use and disclosure of protected health information be limited by the terms of the business partner's contractual agreement with the covered entity. We propose that a contract between a covered entity and a business partner could not grant the business partner authority to make uses or disclosures of protected health information that the covered entity itself would not have the authority to make. The contract between a covered entity and a business partner could further limit the business partner's authority to use or disclose protected health information as agreed to by the parties. Further, the business partner would have to apply the same limitations to its subcontractors (or persons with similar arrangements) who assist with or carry out the business partner's activities.

To help ensure that the uses and disclosures of business partners would be limited to those recognized as appropriate by the covered entities from whom they receive protected health information, subject to the exception discussed below, we are proposing that covered entities be prohibited from disclosing protected health information to a business partner unless the covered entity has entered into a written contract with the business partner that meets the requirements of this subsection. See proposed § 164.506(e)(2)(i). The written contract between a covered entity and a business partner would be required to:

- Prohibit the business partner from further using or disclosing the protected health information for any purpose other than the purpose stated in the contract.
- Prohibit the business partner 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. As discussed above, the covered entity could not permit the business partner to make uses or disclosures that the covered entity could not make.
- Require the business partner to maintain safeguards as necessary to ensure that the protected health information is not used or disclosed except as provided by the contract. We are only proposing a general requirement; the details can be negotiated to meet the particular needs of each arrangement. For example, if the business partner is a two-person firm the contractual provisions regarding safeguards may focus on controlling physical access to a computer or file drawers, while a contract with a business partner with 500 employees would address use of electronic technologies to provide security of electronic and paper records.
- Require the business partner to report to the covered entity any use or disclosure of the protected health information of which the business partner becomes aware that is not provided for in the contract.
- Require the business partner 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 partner with respect to such information.
- Establish how the covered entity would provide access to protected health information to the subject of that information, as would be required under § 164.514, when the business partner has made any material alteration in the information. The covered entity and the business partner would determine in advance how the covered entity would know or could readily ascertain, when a particular individual's protected health information has been materially altered by the business partner, and how the covered entity could provide access to such information.
- Require the business partner 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 HHS or its agents for the purposes of enforcing the provisions of this rule.
- Establish how the covered entity would provide access to protected health information to the subject of that information, as would be required under § 164.514, in circumstances where the business partner will hold the protected health information and the covered entity will not.
- Require the business partner to incorporate any amendments or corrections to protected health information when notified by the covered entity that the information is inaccurate or incomplete.
- At termination of the contract, require the business partner to return or destroy all protected health information received from the covered entity that the business partner still maintains in any form to the covered entity and prohibit the business partner from retaining such protected health information in any form.
- 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 partner has repeatedly violated a term of the contract required by this paragraph.

Each specified contract term above would be considered a separate implementation specification under this proposal for situations in which a

contract is required, and, as discussed below, a covered entity would be responsible for assuring that each such implementation standard is met by the business partner. See proposed § 164.506(e)(2). The contract could include any additional arrangements that do not violate the provisions of this regulation.

The contract requirement that we are proposing would permit covered entities to exercise control over their business partners' activities and provide documentation of the relationship between the parties, particularly the scope of the uses and disclosures of protected health information that business partners could make. The presence of a contract also would formalize the relationship, better ensuring that key questions such as security, scope of use and disclosure, and access by individuals are adequately addressed and that the roles of the respective parties are clarified. Finally, a contract can bind the business partner to return any protected health information from the covered entity when the relationship is terminated.

In lieu of a contracting requirement, we considered imposing only affirmative duties on covered entities to ensure that their relationships with business partners conformed to the standards discussed in the previous paragraph. Such an approach could be considered less burdensome and restrictive, because we would be leaving it to the parties to determine how to make the standards effective. We rejected this approach primarily because we believe that in the vast majority of cases, the only way that the parties could establish a relationship with these terms would be through contract. We also determined that the value of making the terms explicit through a written contract would better enable the parties to know their roles and responsibilities, as well as better enable the Secretary to exercise her oversight role. In addition, we understand that most covered entities already enter into contracts in these situations and therefore this proposal would not disturb general business practice. We invite comment on whether there are other contractual or non-contractual approaches that would afford an adequate level of protection to individuals' protected health information. We also invite comment on the specific provisions and terms of the proposed approach.

We are proposing one exception to the contracting requirement: when a covered entity consults with or makes a referral to another covered entity for the treatment of an individual, we would propose that the sharing of protected health information pursuant to that consultation or referral not be subject to the contracting requirement described above. See proposed § 164.506(e)(1)(i). Unlike most business partner relationships, which involve the systematic sharing of protected health information under a business relationship, consultation and referrals for treatment occur on a more informal basis among peers, and are specific to a particular individual. Such exchanges of information for treatment also appear to be less likely to raise concerns about further impermissible use or disclosure, because health care providers receiving such information are unlikely to have a commercial or other interest in using or disclosing the information. We invite comment on the appropriateness of this exception, and whether there are additional exceptions that should be included in the final regulation.

We note that covered health care providers receiving protected health information for consultation or referral purposes would still be subject to this rule, and could not use or disclose such protected health information for a purpose other than the purpose for which it was received (i.e., the consultation or referral). Further, we note 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 has agreed to impose (e.g., the disclosing provider has provided notice to its patients that it will not make disclosures for research).

Under the system that we are proposing, business partners (including business partners that are covered entities) that have contracts with more than one covered entity would have 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 partner must be authorized through the contract or arrangement with each covered entity that supplied the protected health information to combine or aggregate the information. For example, a business partner of a health plan would be permitted to disclose information to another health plan for coordination of benefits purposes, if such a disclosure were authorized by the business partner's contract with the covered entity that provided the protected health information. However, a business partner that is performing an audit of a group medical practice on behalf of several health plans could not combine protected health information that it had received from each of the plans, even if the business partner's contracts with the plans attempted to allow such activity, because the plans themselves would not be permitted to exchange protected health information for such a purpose. A covered entity would not be permitted to obtain protected health information through a business partner that it could not otherwise obtain itself.

We further note that, as discussed above in section II.C.4, under our proposal a business partner generally could create a database of de-identified health information drawn from the protected health information of more than one covered entity with which it does business, and could use and disclose information and analyses from the database as they see fit, as long as there was no attempt to re-identify the data to create protected health information. In the example from the preceding paragraph, the business partner could review the utilization patterns of a group medical practice on behalf of several groups of plans by establishing a data base of de-identified health information drawn from all of its contracts with covered entities and review the use patterns of all of the individuals in the data base who had been treated by the medical group. The results of the analyses could be used by or distributed to any person, subject to the limitation that the data could not be identified. We would caution that business partners releasing such information and analyses would need to ensure that they do not inadvertently disclose protected health information by releasing examples or discussing specific cases in such a way that the information could be identified by people receiving the analysis or report.

c. *Accountability.* We are proposing that covered entities be accountable for the uses and disclosures of protected health information by their business partners. A covered entity would be 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 partner and it failed to take reasonable steps to cure the breach or terminate the contract. See proposed § 164.506(e)(2)(iii). A covered entity that is aware of impermissible uses and disclosures by a business partner would be responsible for taking such steps as are necessary to prevent further improper use or disclosures and, to the extent practicable, for mitigating any harm caused by such violations.

This could include, for example, requiring the business partner to retrieve inappropriately disclosed information (even if the business partner must pay for it) as a condition of continuing to do business with the covered entity. A covered entity that knows or should know of impermissible use of protected health information by its business partner and fails to take reasonable steps to end the breach would be in violation of this rule.

Where a covered entity acts as a business partner to another covered entity, the covered entity that is acting as business partner would also be responsible for any violations of the regulation.

We considered requiring covered entities to terminate relationships with business partners if the business partner committed a serious breach of contact terms required by this subsection or if the business partner exhibited a pattern or practice of behavior that resulted in repeated breaches of such terms. We rejected that approach because of the substantial disruptions in business relationships and customer service when terminations occur. We instead require the covered entity to take reasonable steps to end the breach and mitigate its effects. We would expect covered entities to terminate the arrangement if it becomes clear that a business partner cannot be relied upon to maintain the privacy of protected health information provided to it. We invite comments on our approach here and whether requiring automatic termination of business partner contracts would be warranted in any circumstances.

We also considered imposing more strict liability on covered entities for the actions of their business partners, just as principals are strictly liable for the actions of their agents under common law. We decided, however, that this could impose too great a burden on covered entities, particularly small providers. We are aware that, in some cases, the business partner will be larger and more sophisticated with respect to information handling than the covered entity. Therefore we instead opted to propose that covered entities monitor use of protected health information by business partners, and be held responsible only when they knew or reasonably should have known of improper use of protected health information.

Our intention in this subsection is to recognize the myriad business relationships that currently exist and to ensure that when they involve the exchange of protected health information, the roles and responsibilities of the different parties with respect to the protected health information are clear. We do not propose to fundamentally alter the types of business relationships that exist in the health care industry or the manner in which they function. We request comments on the extent to which our proposal would disturb existing contractual or other arrangements among covered entities and business partners.

6. Application to Information About Deceased Persons (§ 164.506(f))

[Please label comments about this section with the subject: ''Deceased persons'']

We are proposing that information otherwise protected by these regulations retain that protection for two years after the death of the subject of the information. The only exception that we are proposing is for uses and disclosures for research purposes.

HIPAA includes no temporal limitations on the application of the privacy protections. Although we have the authority to protect individually identifiable health information maintained by a covered entity indefinitely, we are proposing that the requirements of this rule generally apply for only a limited period, as discussed below. In traditional privacy law, privacy interests, in the sense of the right to control use or disclosure of information about oneself, cease at death. However, good arguments exist in favor both of protecting and not protecting information about the deceased. Considering that one of the underlying purposes of health information confidentiality is to encourage a person seeking treatment to be frank in the interest of obtaining care, there is good reason for protecting information even after death. Federal agencies and others sometimes withhold sensitive information, such as health information, to protect the privacy of surviving family members. At the same time, perpetual confidentiality has serious drawbacks. If information is needed for legitimate purposes, the consent of a living person legally authorized to grant such consent must be obtained, and the further from the date of death, the more difficult it may be to identify the person. The administrative burden of perpetual protection may eventually outweigh the privacy interests served.

The proposed two-year period of confidentiality, with an exception for uses and disclosures for research purposes, would preserve dignity and respect by preventing uncontrolled disclosure of information immediately after death while allowing access to the information for proper purposes during this period and for any purpose thereafter. We would not subject the use or disclosure of protected health information of deceased individuals to the requirements in proposed § 164.510(j) governing most uses and disclosures for research because we believe that it is important to remain as consistent as possible with the Common Rule. The Common Rule does not consider deceased persons to be ''human subjects'' and therefore they have never been covered in the standard research protocol assessments conducted under the Common Rule. The Department of Health and Human Services will examine this issue in the context of an overall assessment of the Common Rule. Pending the outcome of this examination, we concluded that this exception was warranted so as not to interfere with standard research practice. We invite comments on whether the exception that we are proposing is necessary, or whether existing research using the protected health information of deceased individuals could proceed under the requirements of proposed § 164.510(j).

Under our proposal, and subject to the exceptions discussed above, the right to control the individual's health information within that two-year time period would be held by an executor or administrator, or in the absence of such an officer, by next-of-kin, as determined under applicable law, or in absence of both, by the holder of the health information. This is reflected in the proposed definition of ''individual'' discussed above. The legally authorized representative would make decisions for the individual with regard to uses or disclosures of the information for purposes not related to treatment, payment or health care operations. Likewise, an authorized representative could exercise the individual rights of inspection, copying, amendment or correction under proposed §§ 164.514 and 164.516.

Under our proposal, information holders could choose to keep information confidential for a longer period. These proposed rules also would not override any legally required prohibitions on disclosure for longer periods.

One area of concern regarding the proposed two-year period of protection relates to information on individual genetic make-up or individual diseases and conditions that may be hereditary. Under the proposed rules, covered entities would be legally allowed to use such information or to disclose records to others, such as commercial collectors

of information, two years after the death of the individual. Since genetic information about one family member may reveal health information about other members of that family, the health data confidentiality of living relatives could be compromised by such uses or disclosures. Likewise, information regarding the hereditary diseases or conditions of the deceased person may reveal health information about living relatives. In the past, information that may not have been legally protected was *de facto* protected for most people because of the difficulty of its collection and aggregation. With the dramatic proliferation of large electronic databases of information about individuals, growing software-based intelligence, and the declining cost of linking information from disparate sources, such information could now be more readily and cost-effectively accessed.

While various State laws have been passed specifically addressing privacy of genetic information, there is currently no federal legislation that deals with these issues. We considered extending the two-year period for genetic and hereditary information, but were unable to construct criteria for protecting the possible privacy interests of living children without creating extensive burden for information holders and hampering health research. We invite comments on whether further action is needed in this area and what types of practical provisions may be appropriate to protect genetic and hereditary health information.

7. Adherence to the Notice of Information Practices (§ 164.506(g))

[Please label comments about this section with the subject: ''Adherence to notice'']

In § 164.506(g), we are proposing that covered plans and providers be required to adhere to the statements reflected in the notice of information practices that would be required under proposed § 164.512. In binding covered plans and providers to their notices, we intend to create a system where open and accurate communication between entities and individuals would become necessary and routine. The corollary to this general rule is that the covered plan or provider would be permitted to modify its notice at any time.

The information practices reflected in the most recent notice would apply to all protected health information regardless of when the information was collected. For example, if information was collected during a period when the notice stated that no disclosures would be made to researchers, and the covered plan or provider later decided that it wanted to disclose information to researchers, the entity would then need to revise its notice. The entity would be permitted to disclose all of the information in its custody to researchers as long as the notice is revised and re-distributed as provided below in § 164.512. We considered permitting a covered entity to change its information practices only with respect to protected health information obtained after it revised its notice. Such a requirement would ensure individuals that the notice they received when they disclosed information to the covered entity would continue to apply to that information. We rejected that approach because compliance with such a standard would require covered entities to segregate or otherwise mark information to be based on the information practices that were in effect at different times. Such an approach would make covered entities extremely reluctant to revise the information practices, and otherwise would be extremely burdensome to administer.

We are concerned that by requiring covered plans and providers to adhere to the practices reflected in their notice, we would encourage entities to create broad, general notices so that all possible uses, disclosures and other practices would be included. Such broad notices would not achieve the goals of open and accurate communication between entities and individuals. We welcome comments on this requirement and alternative proposals to achieve the same goals.

8. Application to Covered Entities That Are Components of Organizations That Are Not Covered Entities

[Please label comments about this section with the subject: ''Component entities'']

In this section we describe how the provisions of this proposed rule apply to persons or organizations that provide health care or have created health plans but are primarily engaged in other unrelated activities. Examples of such organizations include schools that operate on-site clinics, employers who operate self-funded health plans, and information processing companies that include a health care services component. The health care component (whether or not separately incorporated) of the organization would be the covered entity. Therefore, any movement of protected health information into another component of the organization would be a ''disclosure,'' and would be lawful only if such disclosure would be authorized by this regulation. In addition, we propose to require such entities to create barriers to prevent protected health information from being used or disclosed for other activities not authorized or permitted under these proposed rules.

For example, schools frequently employ school nurses or operate on-site clinics. In doing so, the nurse or clinic component of the school would be acting as a provider, and must conform to this proposed rule. School clinics would be able to use protected health information obtained in an on-site clinic for treatment and payment purposes, but could not disclose it to the school for disciplinary purposes except as permitted by this rule. Similarly, an employee assistance program of an employer could meet the definition of ''provider,'' particularly if health care services are offered directly by the program. Protected health information obtained by the employee assistance program could be used for treatment and payment purposes, but not for other purposes such as hiring and firing, placement and promotions, except as may be permitted by this rule.

D. Uses and Disclosures With Individual Authorization (§ 164.508)

[Please label comments about this section With the subject: ''Individual authorization'']

This section addresses the requirements that we are proposing when protected health information is disclosed pursuant to the individual's explicit authorization. The regulation would require that covered entities have authorization from individuals before using or disclosing their protected health information for any purpose not otherwise recognized by this regulation. Circumstances where an individual's protected health information may be used or disclosed without authorization are discussed in connection with proposed §§ 164.510 and 164.522 below.

This section proposes different conditions governing such authorizations in two situations in which individuals commonly authorize covered entities to disclose information:

- Where the individual initiates the authorization because he or she wants a covered entity to disclose his or her record, and
- Where a covered entity asks an individual to authorize it to disclose or use information for purposes other than treatment, payment or health care operations.

In addition, this section proposes conditions where a covered entity or the individual initiates an authorization for use or disclosure of psychotherapy notes or research information unrelated

to treatment. See discussion above in section II.C.1.c.

Individually identifiable health information is used for a vast array of purposes not directly related to providing or paying for an individual's health care. Examples of such uses include targeted marketing of new products and assessing the eligibility of an individual for certain public benefits or for commercial products based on their health status. Under these rules, these types of uses and disclosures could only be made by a covered entity with the specific authorization of the subject of the information. The requirements proposed in this section are not intended to interfere with normal uses and disclosures of information in the health care delivery or payment process, but only to permit control of uses extraneous to health care. The restrictions on disclosure that the regulation would apply to covered entities may mean that some existing uses and disclosures of information could take place only if the individual explicitly authorized them under this section.

Authorization would be required for these uses and disclosures because individuals probably do not envision that the information they provide when getting health care would be disclosed for such unrelated purposes. Further, once a patient's protected health information is disclosed outside of the treatment and payment arena, it could be very difficult for the individual to determine what additional entities have seen, used and further disclosed the information. Requiring an authorization from the patient for such uses and disclosures would enhance individuals' control over their protected health information.

We considered requiring a uniform set of requirements for all authorizations, but concluded that it would be appropriate to treat authorizations initiated by the individual differently from authorizations sought by covered entities. There are fundamental differences in the uses of information and in the relationships and understandings among the parties in these two situations. When individuals initiate authorizations, they are more likely to understand the purpose of the release and to benefit themselves from the use or disclosure. When a covered entity asks the individual to authorize disclosure, we believe the entity should make clear what the information will be used for, what the individual's rights are, and how the covered entity would benefit from the requested disclosure.

Individuals seek disclosure of their health information 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 where health is relevant. Another common instance is tort litigation, where 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.

There could also be circumstances where the covered entity asks an individual to authorize use or disclosure of information, for example to disclose it to a subsidiary to market life insurance to the individual. Similarly, the covered entity might ask that the individual authorize it to send information to a person outside that covered entity—possibly another covered entity or class of covered entity—for purposes outside of treatment, payment, or health care operations. See proposed § 164.508(a)(2)(ii).

1. Requirements When the Individual Has Initiated the Authorization

We are proposing several requirements that would have to be met in the authorization process when the individual has initiated the authorization.

The authorization would have to include a description of the information to be used or disclosed with sufficient specificity to allow the covered entity to know to which information the authorization references. For example, the authorization could include a description of ''laboratory results from July 1998'' or ''all laboratory results'' or ''results of MRI performed in July 1998.'' The covered entity would 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 would not be permitted unless the covered entity were able to clarify the request.

We are proposing no limitations on the information to be disclosed. If an individual wishes to authorize a covered entity to disclose his or her entire medical record, the authorization could so specify. But in order for the covered entity to disclose the entire medical record, the authorization would have be specific enough to ensure that individuals have a clear understanding of what information is to be disclosed under the circumstances. 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 would need to specify ''all health information.''

We would note that our proposal does not require a covered entity to disclose information pursuant to an individual's authorization. Therefore individuals may face reluctance on the part of covered entities that receive authorizations requiring them to classify and selectively disclose information when they do not benefit from the activity. Individuals would need to consider this when specifying the information in the authorization. Covered entities may respond to requests to analyze and separate information for selective disclosure by providing the entire record to the individual, who may then redact and release the information to others.

We do not propose to require an authorization initiated by an individual to state a purpose. When the individual has initiated the authorization, the entity would not need to know why he or she wants the information disclosed. Ideally, anyone asking an individual to authorize release of individually identifiable health information would indicate the purpose and the intended uses. We are unable to impose requirements on the many entities that make such requests, and it would not be feasible to ask covered entities to make judgments about intended uses of records that are disclosed. In the absence of legal controls in this situation, the prudent individual would obtain a clear understanding of why the requester needs the information and how it would be used.

We are proposing that the authorization would be required to identify sufficiently the covered entity or covered entities that would be authorized to use or disclose the protected health information by the authorization. Additionally, the authorization would be required to identify the person or persons that would be authorized to use or receive the protected health information with sufficient specificity to reasonably permit a covered entity responding to the authorization to identify the authorized user or recipient. When an authorization permits a class of covered entities to disclose information to an authorized person, each covered entity would need to know with reasonable certainty that the individual intended for it to release protected health information under the authorization.

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 provided 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. Such an authorization would be permissible (subject to the other requirements of this part) if it sufficiently identifies the government entity as the recipient of the disclosures and it sufficiently identifies the health care providers who would be authorized to release the individual's protected health information under the authorization.

We are proposing that the authorization must state a specific expiration date. We considered providing an alternative way of describing the termination of the authorization, such as ''the conclusion of the clinical trial,'' or ''upon acceptance or denial of this application for life insurance'' (an ''event''), but we are concerned that covered entities could have difficulty implementing such an approach. We also considered proposing that if an expiration date were indicated on the authorization, it be no more than two or three years after the date of the signature. We are soliciting comment on whether an event can be a termination specification, and whether this proposed rule should permit covered entities to honor authorizations with ''unlimited'' or extremely lengthy expiration dates or limit it to a set term of years, such as two or three years.

We are proposing that the authorization include a signature or other authentication (e.g., electronic signature) and the date of the signature. If the authorization is signed by an individual other than the subject of the information to be disclosed, that individual would have to indicate his or her authority or relationship with the subject.

The authorization would also be required to include a statement that the individual understands that he or she may revoke an authorization except to the extent that action has been taken in reliance on the authorization.

When an individual authorizes disclosure of health information to other than a covered entity, the information would no longer be protected under this regulation once it leaves the covered entity. Therefore, we propose that the authorization must clearly state that the individual understands that when the information is disclosed to anyone except a covered entity, it would no longer be protected under this regulation.

We understand that the requirements that we are imposing here would make it quite unlikely that an individual could actually initiate a completed authorization, because few individuals would know to include all of these elements in a request for information. We understand that in most instances, individuals accomplish authorizations for release of health records by completing a form provided by another party, either the ultimate recipient of the records (who may have a form authorizing them to request the records from the record holders) or a health care provider or health plan holding the records (who may have a form that documents a request for the release of records to a third party). For this reason, we do not believe that our proposal would create substantial new burdens on individuals or covered entities in cases when an individual is initiating an authorized release of information. We invite comment on whether we are placing new burdens on individuals or covered entities. We also invite comment on whether the approach that we have proposed provides sufficient protection to individuals who seek to have their protected health information used or disclosed.

2. Requirements When the Covered Entity Initiates the Authorization

We are proposing that when covered entities initiate the authorization by asking individuals to authorize disclosure, the authorization be required to include all of the items required above as well as several additional items. We are proposing additional requirements when covered entities initiate the request for authorization because in many cases it could be the covered entity, and not the individual, that achieves the primary benefit of the disclosure. We considered permitting covered entities to request authorizations with only the basic features proposed for authorizations initiated by the individual, for the sake of simplicity and consistency. However, we believe that additional protections would be merited when the entity that provides or pays for health care requests an authorizations to avert possible coercion.

When a covered entity asks an individual to sign an authorization, we propose to require that it provide on the authorization a statement that identifies the purposes for which the information is sought as well as the proposed uses and disclosures of that information. The required statements of purpose would provide individuals with the facts they need to make an informed decision as to whether to allow release of the information. Covered entities and their business partners would be bound by the statements provided on the authorization, and use or disclosure by the covered entity inconsistent with the statement would constitute a violation of this regulation. We recognize that the covered entities cannot know or control uses and disclosures that will be made by persons who are not business partners to whom the information is properly disclosed. As discussed above, authorizations would need to notify individuals that when the information is disclosed to anyone except a covered entity, it would no longer be protected under this regulation.

We propose to require that authorizations requested by covered entities be narrowly tailored to authorize use or disclosure of only the protected health information necessary to accomplish the purpose specified in the authorization. The request would be subject to the minimum necessary requirement as discussed in section II.C.2. We would prohibit the use of broad or blanket authorizations requesting the use or disclosure of protected health information for a wide range of purposes. Both the information that would be used or disclosed and the specific purposes for such uses or disclosures would need to be specified in the notice.

We are proposing that when covered entities ask individuals to authorize use or disclosure for purposes other than for treatment, payment, or health care operations, they be required to advise individuals that they may inspect or copy the information to be used or disclosed as provided in proposed § 164.514, that they may refuse to sign the authorization, and that treatment and payment could not be conditioned on the patient's authorization. For example, a request for authorization to use or disclose protected health information for marketing purposes would need to clearly state that the individual's decision would have no influence on his or her health care treatment or payment. In addition, we are proposing that when a covered entity requests an authorization, it must provide the individual with a copy of the signed authorization form.

Finally, we are proposing that when the covered entity initiates the authorization and the covered entity would be receiving financial or in-kind compensation in exchange for using or disclosing the health information, the authorization would include a statement that the disclosure would result in commercial gain to the covered entity. For example, a health plan may wish to sell or rent its enrollee mailing list. A pharmaceutical company may offer a provider a discount on its products if

the provider can obtain authorization to disclose the demographic information of patients with certain diagnoses so that the company can market new drugs to them directly. A pharmaceutical company could pay a pharmacy to send marketing information to individuals on its behalf. Each such case would require a statement that the requesting entity will gain financially from the disclosure.

We considered requiring a contract between the provider and the pharmaceutical company in this type of arrangement, because such a contract could enhance protections and enforcement options against entities who violate these rules. A contract also would provide covered entities a basis to enforce any limits on further use or disclosures by authorized recipients. Although we are not proposing this approach now, we are soliciting comment on how best to protect the interests of the patient when the authorization for use or disclosure would result in commercial gain to the covered entity.

3. Model Forms

Covered entities and third parties that wish to have information disclosed to them would need to prepare forms for individuals to use to authorize use or disclosure. A model authorization form is displayed in Appendix to this proposed rule. We considered presenting separate model forms for the two different types of authorizations (initiated by the individual and not initiated by the individual). However, this approach could be subject to misuse and be confusing to covered entities and individuals, who may be unclear as to which form is appropriate in specific situations. The model in the appendix accordingly is a unitary model, which includes all of the requirements for both types of authorization.

4. Plain Language Requirement

We are proposing that all authorizations must be written in plain language. If individuals cannot understand the authorization they may not understand the results of signing the authorization or their right to refuse to sign. See section II.F.1 for more discussion of the plain language requirement.

5. Prohibition on Conditioning Treatment or Payment

We propose that covered entities be prohibited, except in the case of clinical trial as described below, from conditioning treatment or payment for health care on obtaining an authorization for purposes other than treatment, payment or health care operations. This is intended to prevent covered plans and providers from coercing individuals into signing an authorization for a disclosure that is not necessary for treatment, payment or health care operations. For example, a 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 propose one exception to this provision: health care providers would be permitted to condition treatment provided as part of a clinical trial on obtaining an authorization from the individual that his or her protected health information could be used or disclosed for research associated with such clinical trial. 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 participation in the trial on the individual's willingness to authorize that his or her protected health information be used or disclosed for research associated with the trial. We note that the uses and disclosures would be subject to the requirements of § 164.510(j) below.

Under the proposal, a covered entity would not be permitted to obtain an authorization for use or disclosure of information for treatment, payment or health care operations unless required by applicable law. Where such an authorization is required by law, however, it could not be combined in the same document with an individual authorization to use or disclosure of protected health information for any purpose other than treatment, payment or health care operations (e.g., research). We would require that a separate document be used to obtain any other individual authorizations to make it clear to the individual that providing an authorization for such other purpose is not a condition of receiving treatment or payment.

6. Inclusion in the Accounting and Disclosures

As discussed in section II.H.6, we propose that covered entities be required to keep a record of all disclosures for purposes other than treatment, payment or health care operations, including those made pursuant to authorization. In addition, we propose that when an individual requests such an accounting or requests a copy of a signed authorization form, the covered entity must give a copy to the individual. See proposed § 164.515.

7. Revocation of an Authorization by the Individual

We are proposing that an individual be permitted to revoke an authorization at any time except to the extent that action has been taken in reliance on the authorization. See proposed § 164.508(e). That is, an individual could change her or his mind about an authorization and cancel it, except that she or he could not thereby prevent the use or disclosure of information if the recipient has already acted in reliance on the authorization. For example, an individual might cancel her or his authorization to receive future advertisements, but the entity may be unable to prevent mailing of the advertisements that the covered entity or third party has already prepared but not yet mailed.

An individual would revoke the old authorization and sign a new authorization when she or he wishes to change any of the information in the original authorization. Upon receipt of the revocation, the covered entity would need to stop processing the information for use or disclosure to the greatest extent practicable.

8. Expired, Deficient, or False Authorization

The model authorization form or a document that includes the elements set out at proposed § 164.508 would meet the requirements of this proposed rule and would have to be accepted by the covered entity. Under § 164.508(b), there would be no ''authorization'' within the meaning of the rules proposed below if the submitted document has any of the following defects:

- The date has expired;
- On its face it substantially fails to conform to any of the requirements set out in proposed § 164.508, because it lacks an element;
- It has not been filled out completely. Covered entities may not rely on a blank or incomplete authorization;
- The authorization is known to have been revoked; or
- The information on the form is known by the person holding the records to be materially false.

We understand that it would be difficult for a covered entity to confirm the identity of the person who signed the authorization. We invite comment 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.

E. Uses and Disclosures Permitted Without Individual Authorization (§ 164.510)

[Please label comments about this section with the subject: ''Introduction to uses and disclosures without individual authorization'']

This section describes uses and disclosures of protected health information that covered entities could make for purposes other than treatment, payment, and health care operations without individual authorization, and the conditions under which such uses and disclosures could be made. We propose to allow covered entities to use or disclose protected health information without individual authorization for such purposes if the use or disclosure would comply with the applicable requirements of this section.

These categories of allowable uses and disclosures are designed to permit and promote key national health care priorities, and to ensure that the health care system operates smoothly. For each of these categories, this rule would permit—but not require—the covered entity to use or disclose protected health information without the individual's authorization. Some covered entities could conclude that the records they hold, or portions of them, should not be used or disclosed for one or more of these permitted purposes without individuals' authorization (absent a law mandating such disclosure), even under the conditions imposed here. The proposed regulation is intended to reflect the importance of safeguarding individuals' confidentiality, while also enabling important national priority activities that require protected health information.

We considered permitting uses and disclosures only where law affirmatively requires the covered entity to use or disclose protected health information. However, because the activities described below are so important to the population as a whole, we decided to permit a covered entity to use or disclose information to promote those activities even when such activities are not legally mandated. In some cases, however, we would permit a use or disclosure only when such use or disclosure is authorized by other law. The requirements for verification of legal authority are discussed in each relevant section.

Where another law forbids the use or disclosure of protected health information without the individual's authorization, nothing in this section would permit such use or disclosure.

Other law may require use or disclosure of protected health information. If such a use or disclosure is not otherwise addressed in proposed § 164.510(b) through (m), we would in proposed § 164.510(n) permit covered entities to use or disclose protected health information without individual authorization pursuant to any law that mandates such use or disclosure. To be in compliance with this rule, the covered entity must meet the requirements of such other law requiring the use or disclosure. Similarly, nothing in this rule would provide authority for a covered entity to restrict or refuse to make a use or disclosure mandated by other law.

The HIPAA legislative authority generally does not bring the entities that receive disclosures pursuant to this section, including public health authorities, oversight and law enforcement agencies, researchers, and attorneys, under the jurisdiction of this proposed rule. We therefore generally cannot propose restrictions on the further use and disclosure of protected health information obtained by the recipients of these disclosures (unless the recipient is also a covered entity). We believe, however, that in most instances it is sound policy to restrict further uses and disclosures of such protected health information. For example, the Secretary's Recommendations proposed that protected health information obtained by researchers not be further disclosed except for emergency circumstances, for a research project that meets certain conditions, and for oversight of research. We believe that federal legislation should include appropriate restrictions on further use and disclosure of protected health information received by entities for purposes such as those described in this section. We note that, under S.578 (introduced by Senator Jeffords), protected health information disclosed for oversight could not be used against the subject of the protected health information unless the action arises out of and is directly related to a health care fraud or a fraudulent claim for benefits, unless such use is judicially authorized. We believe such safeguards strike the right balance between encouraging national priority oversight activities and protecting individuals' privacy.

The provisions of this section contain requirements related to use and requirements related to disclosure, as appropriate to each of the purposes discussed. For many of these purposes, only requirements relating to disclosure are proposed because there are no appropriate internal uses for such a purpose. Examples include disclosures for next-of-kin and disclosures for banking and financial purposes.

For many of these permitted disclosures, we would require the covered entity to verify the identity of the requestor and his or her legal authority to make the request. Requirements for verifying the identity and authority of requests for information are further discussed in II.G, ''Administrative Requirements.'' As discussed in more detail in section II.G.3. of this preamble, the verification requirement would apply where the identity of the person making the request is not already known to the covered entity (e.g., where the disclosure is not part of a routine business transaction). We would ask health plans and health care providers to take reasonable steps to verify the identity of persons requesting protected health information, such as asking to see a badge or other proof of the identity of government officials, and would allow covered entities to rely on the statement of government officials and others regarding the legal authority for the activity. We would not require covered entities to make an independent inquiry into the legal authority behind requests for protected health information.

The provisions below would permit covered entities to use or disclose protected health information without individual authorization, pursuant to certain requirements. Although health care clearinghouses would be defined as covered entities under this rule, in most instances clearinghouses will be receiving and maintaining protected health information as the business partner of a covered health plan or provider. In such cases, proposed § 164.510(a)(2) provides that the clearinghouses that hold protected health information as business partners would not be permitted to make uses or disclosures otherwise permitted by this section unless such uses or disclosures also were permitted under the terms of the contract between the clearinghouse and the business partner.

1. Uses and Disclosures for Public Health Activities (§ 164.510(b))

[Please label comments about this section with the subject: ''Public health'']

We propose to permit covered entities to disclose protected health information without individual authorization to public health authorities carrying out public health activities authorized by law, to non-governmental entities authorized by law to carry out public health activities, and to persons who may be at risk of contracting or spreading a disease (when other law

authorizes notification). Where the covered entity also is a public health agency, such as a public hospital or local health department, it would be permitted to use protected health information in all cases in which it would be permitted to disclose such information for public health activities under this section.

a. *Importance of public health and need for protected health information.* Public health authorities are responsible for promoting health and quality of life by preventing and controlling disease, injury, and disability. Inherent in the collection of information for public health activities is a balancing of individual versus communal interests. While the individual has an interest in maintaining the privacy of his or her health information, public health authorities have an interest in the overall health and well-being of the entire population of their jurisdictions. To accomplish this, public health authorities engage in a number of activities, including: traditional public health surveillance; investigations and interventions with respect to communicable diseases; registries (such as immunization or cancer registries); programs to combat diseases that involve contacting infected persons and providing treatment; and actions to prevent transmission of serious communicable diseases.

Public health activities also include regulatory investigations and interventions such as pre-market review of medical products, and evaluations of the risk-benefit profile of a drug or medical product before and after approval (relying on critical epidemiological techniques and resources such as HMO claims databases and medical records). Public health agencies use the results of analyses to make important labeling changes and take other actions, such as the removal of non-compliant products from the market.

We considered requiring individual authorization for certain public health disclosures, but rejected this approach because many important public health activities would not be possible if individual authorization were required. In the case of contagious diseases, for example, if individual authorization were required before individually identifiable information could be provided to public health workers, many other people who may be harboring contagious diseases may be missed by efforts to halt the spread of disease because they failed to provide the appropriate individual authorization. Their failure to authorize could place the general population at risk for contracting an infectious disease. Furthermore, always requiring individual authorization to disclose protected health information to public health authorities would be impractical due to the number of reports and the variety of sources from which they are made. If individuals were permitted to opt out from having their information included in these public health systems, the number of persons with a particular condition would be undercounted. Furthermore, the persons who did authorize the inclusion of their information in the system might not be representative of all persons with the disease or condition.

We also considered limiting certain public health disclosures to de-identified health information. However, identifiable information could be required in order to track trends in a disease over time, and to assess the safety of medical treatments. While de-identified information could be appropriate for many public health activities, there are also many public health activities that require individual identifiers. We decided not to attempt to define specific public health activities for which only de-identified information could be disclosed, in part because public health data collection requirements would be better addressed in public health laws, and in part to reflect the variation in information technologies available to public health authorities. Instead, we rely on the judgment of public health authorities as to what information would be necessary for a public health activity. See discussion in section II.C.2.

b. *Public health activities.* We intend a broad reading of the term ''public health activities'' to include the prevention or control of disease, injury, or disability. We considered whether to propose a narrow or broad scope of public health activities for which disclosure without individual authorization would be permitted. For the reasons described above, we believe that both the general public and individual interests are best served by a broad approach to public health disclosures.

We therefore propose that covered entities be permitted to disclose protected health information to public health authorities for the full range of public health activities described above, including reporting of diseases, injuries, and conditions, reporting of vital events such as birth and death to vital statistics agencies, and a variety of activities broadly covered by the terms public health surveillance, public health investigation, and public health intervention. These would include public health activities undertaken by the FDA to evaluate and monitor the safety of food, drugs, medical devices, and other products. These terms would be intended to cover the spectrum of public health activities carried out by federal, State, and local public health authorities. The actual authorities and terminology used for public health activities will vary under different jurisdictions. We do not intend to disturb or limit current public health activities.

c. *Permitted recipients of disclosures for public health activities.* Disclosures without individual authorization for public health activities would be permitted to be made to only three types of persons: public health authorities, non-governmental entities authorized by law to carry out public health activities, and persons who may be at risk of contracting or spreading a disease, if other law authorizes notification.

i. *Public health authorities.*

We propose to define ''public health authority'' broadly, based on the function being carried out, not the title of the public entity. Therefore, disclosures under this proposed rule would not be limited to traditional public health entities such as State health departments. Other government agencies and entities carry out public health activities in the course of their missions. For example, the Occupational Safety and Health Administration, the Mine Safety and Health Administration, and the National Institute for Occupational Safety and Health conduct public health investigations related to occupational health and safety. The National Transportation Safety Board investigates airplane and train crashes in an effort to reduce mortality and injury by making recommendations for safety improvements. Similar inquiries are conducted by the military services. The Food and Drug Administration reviews product performance prior to marketing, and investigates adverse events reported after marketing by industries, health professionals, consumers, and others. The Environmental Protection Agency investigates the effects of environmental factors on health. The definition of public health authority reflects the need for access to data and information including protected health information by these other agencies and authorities consistent with their official mandates under applicable law.

ii. *Non-governmental entities carrying out public health activities.*

The proposed rule would further provide that disclosures may be made not only to government agencies, but also to other public and private entities

as otherwise required or authorized by law. For example, this would include tracking medical devices, where the initial disclosure is not to a government agency, but to a device manufacturer that collects information under explicit legal authority, or at the direction of the Food and Drug Administration. Also, the cancer registries mentioned above could be operated by non-profit organizations such as universities funded by public health authorities which receive reports from physicians and laboratories pursuant to State statutory requirements to report.

We considered limiting public health disclosures to only government entities, but the reality of current public health practice is that a variety of activities are conducted by public health authorities in collaboration with non-governmental entities. Federal agencies also use a variety of mechanisms including contracts, grants, cooperative agreements, and other agreements such as memoranda of understanding to carry out and support public health activities. These relationships could be based on specific or general legal authorities. It is not our intent to disturb these relationships. Limiting the ability to collaborate with other entities and designate them to receive protected health information, could potentially have an adverse impact on public health practice.

iii. *Persons who may be at risk of contracting or spreading a disease.*

The proposed rule would allow disclosure to a person who could have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition and is authorized by law to be notified as necessary in the conduct of a public health intervention or investigation. Physicians, in carrying out public health interventions authorized by law, can notify persons who have been exposed to a communicable disease, or who otherwise may be at risk of contracting or spreading a disease or condition. That notification may implicitly or explicitly reveal the identity of the individual with the disease to which the person could have been exposed, but should be permitted as a disclosure in the course of a legally authorized public health intervention or investigation. The proposed rule would not (and, under the HIPAA legislative authority, cannot) impose a confidentiality obligation on the person notified.

d. *Additional requirements.* Under proposed § 164.518(c), covered entities would have to verify the identity of the person requesting protected health information and the legal authority supporting that request, before the disclosure would be permitted under this subsection. Preamble section II.G.3 describes these requirements in more detail.

We note that to the extent that the public health authority is providing treatment as defined in proposed § 164.504, the public health authority would be a covered health care provider for purposes of that treatment, and would be required to comply with this regulation.

We also note that the preemption provision of the HIPAA statute creates a special rule for a subset of public health disclosures: this regulation cannot preempt State law regarding ''public health surveillance, or public health investigation or intervention * * *''.

2. Use and Disclosure for Health Oversight Activities. (§ 164.510(c))

[*Please label comments about this section with the subject: ''Health oversight*'']

In section § 164.510(c), we propose to allow covered entities to disclose protected health information to public oversight agencies (and to private entities acting on behalf of such agencies) without individual authorization, for health oversight activities authorized by law. In cases in which a covered entity is also an oversight agency, it would be permitted to use protected health information in all cases in which it would be permitted to disclose such information for health oversight activities under this section.

a. *Importance of oversight and need for protected health information.* Oversight activities are critical to support national priorities, including combating fraud in the health care industry, ensuring nondiscrimination, and improving the quality of care. The goals of public agencies' oversight activities are: to monitor the fiscal and programmatic integrity of health programs and of government benefit programs; to ensure that payments or other benefits of these programs are being provided properly; to safeguard health care quality; to monitor the safety and efficacy of medical products; and to ensure compliance with statutes, regulations, and other administrative requirements applicable to public programs and to health care delivery.

Oversight activities are a national priority in part because of the losses in the healthcare system due to error and abuse. For example, the HHS Office of Inspector General recently estimated losses due to improper Medicare benefit payments to be about seven percent. See ''Improper Fiscal Year 1998 Medicare Fee-For Service-Payments,'' transmittal from Inspector General June Gibbs Brown to HCFA Administrator Nancy-Ann Min DeParle (February 9, 1999). Similarly, the final report of the President's Advisory Commission on Consumer Protection and Quality in the Health Care Industry concluded that ''employing the extensive knowledge and expertise of organizations that oversee health care quality * * * is essential to quality improvement.'' (http://www.hcqualitycommission.gov/final/chap09.html)

There are certain oversight activities done as statistical inquiries that can be conducted without direct access to individually identifiable health information. However, many instances exist in which government oversight agencies, and private entities under contracting to act on their behalf, need to examine individually identifiable health information to conduct their investigations effectively. For example, to determine whether a hospital has engaged in fraudulent billing practices, it could be necessary to examine billing records for a set of individual cases. Billing abuses are detected by cross-checking the records of specific patients to see the medical documentation in support of a service. 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. Other inquiries require review of individually identifiable health information to identify specific instances of the anomalies in treatment or billing patterns detected in statistical analysis. Even in most statistical inquiries of the type just described, in a paper environment particular patient charts must be examined, and the patient's name would be disclosed because it would be on each page of the chart.

b. *Proposed requirements.* Specifically, we would permit covered entities to disclose protected health information without individual authorization to a health oversight agency to conduct oversight activities authorized by law. Disclosures also could be made to private entities working under a contract with or grant of authority from one or more of the government oversight agencies described above. As discussed below, oversight activities by private entities operating pursuant to contracts with covered entities, such as accreditation organizations, would not be permitted to receive information under this provision, even if accreditation by such an organization is recognized by law as fulfilling a government requirement or

condition of participation in a government program (often referred to as ''deemed status'').

Under our rule, oversight activities would include conducting or supervising the following activities: Audits; investigations; inspections; civil, criminal or administrative proceedings or actions; and other activities necessary for appropriate oversight of the health care system, of government benefit programs for which health information is relevant to beneficiary eligibility, and of government regulatory programs for which health information is necessary for determining compliance with program standards. This regulation does not create any new right of access to health records by oversight agencies, and could not be used as authority to obtain records not otherwise legally available to the oversight agency.

Under our rule, a health oversight agency would be defined as a public agency authorized by law to conduct oversight activities relating to the health care system, a government program for which health information is relevant to determining beneficiary eligibility or a government regulatory program for which health information is necessary for determining compliance with program standards. Examples of agencies in the first category would include 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. Examples of agencies in the second category include the Social Security Administration and the Department of Education. Examples of agencies in the third category include the workplace safety programs such as the Occupational Health and Safety Administration and the Environmental Protection Agency. Agencies that conduct both oversight and law enforcement activities would be subject to this provision when conducting oversight activities.

In cases where health oversight agencies are working in tandem with other agencies overseeing public benefit programs to address compliance, fraud, or other integrity issues that could span across programs, the oversight activities of the team would be considered health oversight and disclosure to and among team members would be permitted under the proposed rule to the extent permitted under other law. For example, a fraud investigation could attempt to find a pattern of abuse across related programs, such as Medicaid and the supplemental security income program. Protected health information could be disclosed to the team of oversight agencies and could be shared among such agencies for oversight activities.

Public oversight agencies sometimes contract with private entities to conduct program integrity activities on a public agency's behalf. Such audits or investigations may include, for example, program integrity reviews of fraud and abuse in billing Federal and State health care programs; investigations conducted in response to consumer complaints regarding the quality or accessibility of a particular provider, health plan, or facility; and investigations related to disciplinary action against a health care provider, health plan, or health care facility. Covered entities may disclose protected health information to these agents to the extent such disclosure would be permitted to the public oversight body.

In many cases today, public agencies' contracts with private entities conducting investigations on their behalf require the private oversight organization to implement safeguards to protect individual privacy. HIPAA does not provide statutory authority to regulate the contracts between public oversight entities and their agents. However, we encourage public oversight entities to include privacy safeguards in all such contracts, and believe it would be appropriate for federal legislation to impose such safeguards.

In developing our proposal, we considered but rejected the option of providing an exemption from the general rules for situations in which a covered entity has a contract with a private accreditation organization to conduct an accreditation inspection. In such instances, the accreditation organization is performing a service for the covered entity much like any other contractor. The situation is not materially different in instances where accreditation from a private organization would have the effect of ''deeming'' the covered entity to be in compliance with a government standard or condition of participation in a government program. In both cases, the accreditation organization is performing a service for the covered entity, not for the government. In our considerations, we were unable to identify a reason that covered entities should hold these contractors to lesser standards than their other contractors. Individuals' privacy interests would not be diminished in this situation, nor is there any reason why such accreditation organizations should not be held to the requirements described above for business partners. Proposed rules for disclosure to these entities are discussed in section II.C.5., ''Application to business partners.'' We invite comment on our proposed approach.

c. *Additional considerations.* We do not propose any new administrative or judicial process prior to disclosure. This regulation would permit disclosure of protected health information without compulsory process where such disclosure is otherwise allowed. However, this regulation also would not abrogate or modify other statutory requirements for administrative or judicial determinations or for other procedural safeguards, nor would it permit disclosures forbidden by other law.

Under this § 164.518(c), covered entities would have an obligation to verify the identity of the person requesting protected health information and the legal authority behind the request before the disclosure would be permitted under this subsection. Preamble section II.G.3. describes these requirements in more detail.

3. Use and Disclosure for Judicial and Administrative Proceedings (§ 164.510(d))

[*Please label comments about this section with the subject: ''Judicial and administrative proceedings''*]

In § 164.510(d), we propose to 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 by a court or administrative tribunal. A court order would not be required if the protected health information being requested relates to a party to the proceeding whose health condition is at issue, or if the disclosure would otherwise be permitted under this rule. A covered entity that also is a government entity would be permitted to use protected health information in a judicial or administrative proceeding under the same conditions that it could make a disclosure of protected health information under this paragraph.

a. *Importance of judicial and administrative process and the need for protected health information.* Protected health information is often needed as part of an administrative or judicial proceeding. Examples of such proceedings would include personal injury or medical malpractice cases or other lawsuits in which the medical condition of a person is at issue, and judicial or administrative proceedings to determine whether an illness or injury was caused by workplace conditions or

exposure to environmental toxins. The information may be sought well before a trial or hearing, to permit the party to discover the existence or nature of testimony or physical evidence, or in conjunction with the trial or hearing, in order to obtain the presentation of testimony or other evidence. These uses of health information are clearly necessary to allow the smooth functioning of the legal system. Requiring the authorization of the subject prior to disclosure could mean that crucial information would not be available, and could be unfair to persons who have been wronged.

b. *Proposed requirements.* We propose to 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 a court order or an order by an administrative law judge specifically authorizing the disclosure of protected health information. The exception to this requirement is where the protected health information being requested relates to a party to the proceeding whose health condition is at issue, and where the disclosure is made pursuant to lawful process (e.g., a discover order) or is otherwise authorized by law. We note that this would not apply where the disclosure would otherwise be permitted under this rule.

The proposed provisions of this section are intended to apply to the broad spectrum of judicial and administrative procedures by which litigants, government agencies, and others request information for judicial or administrative proceedings, including judicial subpoenas, subpoenas duces tecum, notices of deposition, interrogatories, administrative subpoenas, and any disclosure pursuant to the Federal Rules of Civil Procedures, the Federal Rules of Criminal Procedures, comparable rules of other courts (including State, tribunal, or territorial courts) and comparable rules of administrative agencies. Under the rule, a covered entity could not respond to such requests unless they determined that the request is pursuant to a court order authorizing disclosure of protected health information or if the individual who is the subject of the protected health information is a party to the proceeding and his or her medical condition or history is at issue.

Covered entities generally would not be required to conduct any independent investigation of the legality of the process under which the protected health information is being sought, but would need to review the request protected health information to ensure that the disclosure would meet the terms of this provision. Where the request is accompanied by an order from a court, the covered entity could rely on a statement in the order authorizing disclosure of protected health information. The statement could be a general one, indicating that protected health information is relevant to the matter, or it could identify specifically what protected health information may be disclosed. The covered entity could rely on either type of statement, but it could not disclose more information than was authorized by the court where the scope of the authorized disclosure is clear.

Where the request is not accompanied by a court order or order from an administrative law judge, the covered entity would be required to determine whether the request relates to the protected health information of a litigant whose health is at issue, a written statement from the requester certifying that the protected health information being requested is about a litigant to the proceeding and that the health condition of such litigant is at issue at such proceeding. Such a certification could be from the agency requesting the information (e.g., in an administrative proceeding) or from legal counsel representing a party to litigation. We invite comments on whether this requirement is overly burdensome and on whether it is sufficient to protect protected health information from unwarranted disclosures.

We are not proposing to preclude a covered entity from contesting the nature or scope of the process when the procedural rules governing the proceeding so allow and covered entities could well choose to assert privileges against disclosure on behalf of individuals.

In developing our proposal, we considered permitting covered entities to disclose protected health information pursuant to any request made in conjunction with a judicial or administrative proceeding. We rejected this option because we believe that current procedures for document production could result in unwarranted disclosure of protected health information. Under current practice, requests for documents are developed by the parties to a proceeding, with little review or oversight unless the request is challenged by the opposing party. In many instances, the parties make very broad discovery requests that result in the production of large numbers of documents for review. Recipients of broad motions for document production often provide the requester with a substantial quantity of material, expecting the requester to page through the documents to identify the ones that are relevant to the proceeding. While such a process may be appropriate for many types of records, we are concerned that it could lead to substantial breaches of privacy where the material being requested is protected health information. We are unsure if it is appropriate for private attorneys, government officials and others who develop such requests to be able to circumvent the protections provided by this rule with simple motions for document production that have not been subject to third-party review.

Under our proposal, therefore, a party to a proceeding that wishes production of information that includes protected health information would generally need to seek judicial review of the request. If a court determines that a request for protected health information is appropriate to the proceeding, a covered entity can produce the protected health information pursuant to an otherwise lawful request.

We propose an exception to the general requirement for judicial review for protected health information for instances in which the protected health information of a party to the proceeding is relevant to the proceeding. In such instances, the party will have counsel who can object to an overly broad or unwarranted discovery of the party's protected health information or will receive the discovery request directly and, again, will have an opportunity to object prior to disclosure.

We note that there are other existing legal requirements governing the disclosure of protected health information, and which govern the procedures in federal, State and other judicial and administrative proceedings. For example, 42 U.S.C. 290dd–2 and the implementing regulations, 42 CFR part 2, will continue to govern the disclosure of substance abuse patient records. There may also be provisions of a particular State's law governing State judicial or administrative proceedings, including State medical record privacy statutes, as well as precedential court opinions, which apply to the circumstances described in the section, that will not be preempted by this part. Also, the discovery of psychiatric counseling records in federal proceedings governed by section 501 of the Federal Rules of Evidence, has been restricted in certain circumstances, by *Jaffee* v. *Redmond*, 116 S. Ct. 1923 (1996). These more stringent rules would remain in place.

4. Disclosure to Coroners and Medical Examiners (§ 164.510(e))

[*Please label comments about this section with the subject: ''Coroners and medical examiners''*]

In § 164.510(e), we propose to allow covered entities to disclose protected health information without individual authorization to coroners and medical examiners, as authorized by law, for identification of a deceased person or to determine cause of death.

a. Importance of disclosure to coroners and medical examiners and the need for protected health information. Coroners and medical examiners, who under State or other law typically are public officials, have a legitimate need to obtain protected health information in an expeditious manner in order to carry out their legal responsibility to identify deceased persons and determine cause of death. Such disclosure would be clearly in the public interest, and should be included among the types of disclosures for which the public interest in efficient sharing of medical information outweighs any individual privacy interests that may be compromised.

b. *Proposed requirements.* Proposed § 164.510(e) would allow covered entities to disclose protected health information about a deceased person without individual authorization to coroners and medical examiners, consistent with other law, for the purpose of a post-mortem investigation.

We recognize that a deceased person's medical record could include information that potentially could reveal health information about others, for example, relatives who have the same genetically linked disease as the deceased individual. In developing this section of the proposed rule, we considered requiring covered entities to redact any protected health information about persons other than the deceased before giving the record to coroners or medical examiners.

We rejected this option for two reasons. First, coroners and medical examiners typically need significant portions of a deceased person's medical record, and, in some cases, all medical records that are available, to conduct a post-mortem investigation, which may also include an autopsy. Second, they need to obtain the record quickly, because there is a limited time period after death within which an autopsy can be conducted. Requiring covered entities to take the time to review and redact portions of the health information before providing it to a coroner or medical examiner would create delays that could make it impossible to conduct an autopsy appropriately. Nothing in this rule would prohibit a covered entity from undertaking such redaction on its own initiative so long as the information provided would meet the needs of the coroner or medical examiner.

In addition to these two reasons, it is our understanding that health care providers, as a standard record keeping practice, rarely identify specific persons other than the patient in the record. We are soliciting comment on whether health care providers routinely identify other persons specifically in a individual's record and if so, whether we should require the provider to redact the information about the other person before providing it to a coroner or medical examiner.

Under § 164.518(c), covered entities would have an obligation to verify the identity of the coroner or medical examiner making the request for protected health information and the legal authority supporting the request, before the disclosure would be permitted under this subsection. Preamble section II.G.3. describes these requirements in more detail.

We intend to allow only those disclosures that are authorized by other applicable law. Laws vary widely regarding release of health information to coroners and medical examiners for the purposes of identifying deceased persons or determining cause of death, and we do not intend to disturb those practices.

5. Disclosure for Law Enforcement (§ 164.510(f))

[*Please label comments about this section with the subject: ''Law enforcement''*]

In § 164.510(f), we propose to permit covered entities to disclose protected health information without individual authorization to a law enforcement official conducting a law enforcement inquiry authorized by law if the request for protected health information is made pursuant to a judicial or administrative process, as described below. Similarly, we propose to permit covered entities to disclose protected health information to a law enforcement official without individual authorization for the conduct of lawful intelligence activities. We also propose to permit covered entities to disclose protected health information to a law enforcement official about the victim of a crime, abuse or other harm, if the information is needed to determine both whether a violation of law by a person other than the victim has occurred and whether an immediate law enforcement activity might be necessary. We would further permit such disclosure for the purpose of identifying a suspect, fugitive, material witness, or missing person, if the covered entity discloses only limited identifying information. Finally, we would permit disclosure of protected health information by a health plan or a health care provider without individual authorization to law enforcement officials if the plan or provider believed in good faith that the disclosed protected health information would constitute evidence of criminal conduct that constitutes health care fraud, occurred on the premises of the covered entity, or was witnessed by an employee of the covered entity.

i. *Law enforcement need for protected health information.* Law enforcement officials need protected health information for their investigations in a variety of circumstances. Health information about a victim of a crime may be needed to investigate the crime, or to allow prosecutors to determine the proper charge. For some crimes, the severity of the victim's injuries will determine what charge should be brought against a suspect. The medical condition of a defendant could also 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. Medical, billing, accounting or other documentary records in the possession of a covered entity can be important evidence relevant to criminal fraud or conspiracy investigations. Nor is this list of important uses by law enforcement exhaustive.

In many cases, the law enforcement official will obtain such evidence through legal process, such as judicially executed warrant, an administrative subpoena, or a grand jury subpoena. In other circumstances, time constraints preclude use of such process. For example, health information may be needed when a law enforcement official is attempting to apprehend an armed suspect who is rapidly fleeing. 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.

Protected health information could be sought as part of a law enforcement investigation, to determine whether and who committed a crime, or it could be sought in conjunction with the trial to be presented as evidence. These uses of medical information are clearly in the public interest. Requiring the authorization of the subject prior to disclosure could impede important law enforcement activities by making

apprehension and conviction of some criminals difficult or impossible.

As described above, this proposed rule seeks to respond appropriately to new risks to privacy that could emerge as the form of medical records changes in coming years. The administrative simplification mandated by HIPAA will lead to far greater exchanges of individually identifiable health information among covered entities in the future, increasingly in electronic form. If a misperception were to develop that law enforcement had instant and pervasive access to medical records, the goals of this proposed regulation could be undermined. For instance, individuals might become reluctant to seek needed care or might report inaccurately to providers to avoid revealing potentially embarrassing or incriminating information. In addition, popular concerns about government access to sensitive medical records might impede otherwise achievable progress toward administrative simplification. We believe that the proposed prophylactic and administrative rules governing disclosure to law enforcement officials, as described below, are justified in order to avoid these harms in the future.

ii. *Proposed requirements.* In § 164.510(f), we propose to permit covered entities to disclose protected health information to law enforcement officials conducting or supervising a law enforcement inquiry or proceeding authorized by law if the request for protected health information is made:

- Pursuant to a warrant, subpoena, or order issued by a judicial officer;
- Pursuant to a grand jury subpoena;
- Pursuant to an administrative subpoena or summons, civil investigative demand, or similar certification or written order issued pursuant to federal or state law where (i) the records sought are relevant and material to a legitimate law enforcement inquiry; (ii) the request is as specific and narrowly drawn as is reasonably practicable to meet the purposes of the inquiry; and (iii) de-identified information could not reasonably be used to meet the purposes of the inquiry;
- For limited identifying information where necessary to identify a suspect, fugitive, witness, or missing person;
- By a law enforcement official requesting protected health information about an individual who is, or who is suspected to be, the victim of a crime, abuse or other harm, if such law enforcement official represents that (i) such information is needed to determine whether a violation of law by a person other than the victim has occurred and (ii) immediate law enforcement activity which depends on the official obtaining such information may be necessary;
- 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, and the disclosure is otherwise authorized under Federal or state law; or
- To law enforcement officials when a covered entity believes in good faith that the disclosed protected health information constitutes evidence of criminal conduct that: (i) Arises out of and is directly related to the receipt of health care or payment for health care (including a fraudulent claim for health care) or qualification for or receipt of benefits, payments or services based on a fraudulent statement or material misrepresentation of the health of a patient; (ii) occurred on the premises of the covered entity; or (iii) was witnessed by an employee or other workforce member of the covered entity.

In drafting the proposed rule, we have attempted to match the level of procedural protection for privacy with the nature of the law enforcement need for access. Therefore, access for law enforcement under this rule would be easier where other rules would impose procedural protections, such as where access is granted after review by an independent judicial officer. Access would also be easier in an emergency situation or where only limited identifying information would be provided. By contrast, this rule proposes stricter standards for administrative requests, where other rules could not impose appropriate procedural protections.

Under the first part of this proposal, we would authorize disclosure of protected health information pursuant to a request that has been reviewed by a judicial officer. Examples of such requests include State or federal warrants, subpoenas, or other orders signed by a judicial officer. Review by a judicial officer is significant procedural protection for the proper handling of individually identifiable health information. Where such review exists, we believe that it would be appropriate for covered entities to disclose individually identifiable health information pursuant to the order.

Under the second part of this proposal, we would authorize disclosure of protected health information pursuant to a State or federal grand jury subpoena. Information disclosed to a grand jury is covered by significant secrecy protections, such as under Federal Rule of Criminal Procedure 6(e) and similar State laws. Our understanding is that State grand juries have secrecy protections substantially as protective as the federal rule. We solicit comment on whether there are any State grand jury secrecy provisions that are not substantially as protective.

Under the third part of this proposal, we would set somewhat stricter standards than exist today for disclosure pursuant to administrative requests, such as an administrative subpoena or summons, civil investigative demand, or similar process authorized under law. These administrative actions do not have the same procedural protections as review by an independent judicial officer. They also do not have the grand jury secrecy protections that exist under federal and State law. For administrative requests, an individual law enforcement official can define the scope of the request, sometimes without any review by a superior, and present it to the covered entity. We propose, therefore, that a greater showing should be made for an administrative request before the covered entity would be permitted to release protected health information. We also believe that the somewhat stricter test for administrative requests would provide some reason for officials to choose to obtain protected health information through process that includes the protections offered by judicial review or grand jury secrecy.

We therefore propose that a covered entity could disclose protected health information pursuant to an administrative request, issued pursuant to a determination that: (i) The records sought are relevant and material to a legitimate law enforcement inquiry; (ii) the request is as specific and narrowly drawn as is reasonably practicable; and (iii) de-identified information could not reasonably be used to meet the purpose of the request.

Because our regulatory authority does not extend to law enforcement officials, we are seeking comment on how to create an administrable system for implementing this three-part test. We do not intend that this provision require a covered entity to second guess representations by an appropriate law enforcement official that the three part test has been met.

To verify that the three-part test has been met, we propose that a covered entity be permitted to disclose protected health information to an appropriate law enforcement official pursuant to a subpoena or other covered administrative request that on its face indicates that the three-part test has

been met. In the alternative, where the face of the request does not indicate that the test has been met, a covered entity could disclose the information upon production of a separate document, signed by a law enforcement official, indicating that the three-part test has been met. Under either of these alternatives, disclosure of the information can also be made if the document applies any other standard that is as strict or stricter than the three-part test.

This approach would parallel the research provisions of proposed § 164.510(j). Under that section, disclosure would be authorized by a covered entity where the party seeking the records produces a document that states it has met the standards for the institutional review board process. We solicit comments on additional, administrable ways that a law enforcement official could demonstrate that the appropriate issuing authority has determined that the three-part test has been met.

We solicit comment on the burdens and benefits of the proposed three-part test for administrative requests. For covered entities, we are interested in comments on how burdensome it would be to determine whether the three-part test has been met, and we would explore suggestions for approaches that would be more easily administered. For law enforcement, we are interested in the potential impact that this approach might have on current law enforcement practices, and the extent to which law enforcement officials believe that their access to information critical to law enforcement investigations could be impaired. We solicit comment on the burden on law enforcement officials, compared to current practice, of writing the administrative requests. We would also like comments on whether there are any federal, State, or local laws that would create an impediment to application of this section, including the proposed three-part test. If there are such impediments, we would solicit comment on whether extending the effective date of this section could help to prevent difficulties. On the benefit side, we are interested in comments on the specific gains for privacy that would result from requiring law enforcement to comply with greater procedures than currently exist for gaining access to protected health information.

As the fourth part of this proposal, we address limited circumstances where the disclosure of health information by covered entities would not be made pursuant to lawful process such as judicial order, grand jury subpoena, or administrative request. In some cases law enforcement officials could seek limited but focused information needed to obtain a warrant. For example, 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.

In such instances, we propose to permit covered entities to disclose ''limited identifying information'' for purposes of identifying a suspect, fugitive, material witness, or missing person. We would define ''limited identifying information'' as the name, address, social security number, date of birth, place of birth, type of injury, date and time of treatment, and date of death. Disclosure of any additional information would cause the covered entity to be out of compliance with this provision, and subject to sanction. The request for such information could be made orally or in writing. Requiring the request to be in writing could defeat the purposes of this provision. We solicit comment on whether the list of ''limited identifying information'' is appropriate, or whether additional identifiers, such as blood type, also should be permitted disclosures under this section. Alternatively, we solicit comment on whether any of the proposed items on the list are sufficiently sensitive to warrant a legal process requirement before they should be disclosed.

Under the fifth part of the proposal, we would clarify that the protected health information of the victim of a crime, abuse or other harm could be disclosed to a law enforcement official if the information is needed to determine both whether a violation of law by a person other than the victim has occurred and whether an immediate law enforcement activity might be necessary. There could be important public safety reasons for obtaining medical records or other protected health information quickly, perhaps before there would be time to get a judicial order, grand jury subpoena, or administrative order. In particular, where the crime was violent, information about the victim's condition could be needed to present to a judge in a bond hearing in order to keep the suspect in custody while further evidence is sought. Information about the victim also could be important in making an appropriate charging decision. Rapid access to victims' medical records could reduce the risk of additional violent crimes, such as in cases of spousal or child abuse or in situations where the protected health information could reveal evidence of the identity of someone who is engaged in ongoing criminal activities.

In some of these instances, release of protected health information would be authorized under other sections of this proposed regulation, pursuant to provisions for patient consent, health oversight, circumstances, or disclosure pursuant to mandatory reporting laws for gunshot wounds or abuse cases. (As discussed later in section II.I, our rule would not be construed to invalidate or limit the authority, powers or procedures established under any law that provides for reporting of injury, child abuse or death.) In addition, § 164.510(k) addressing emergency circumstances would permit covered entities to disclose protected health information in instances where the disclosure could prevent imminent harm to the individuals or to the public. However, we propose to include this fifth provision for law enforcement access to ensure that immediate need for law enforcement access to information about a victim would be permitted under this rule.

Under the sixth part of this proposal, we seek to assure that this rule would not interfere with the conduct of lawful security functions in protection of the public interest, as defined by the Congress. Therefore, we would allow disclosure of protected health information for the conduct of lawful intelligence activities conducted pursuant to the National Security Act of 1947. Similarly, we would allow disclosure of protected health information for providing protective services to the President or other individuals pursuant to section 3056 of title 18, United States Code. Where such disclosures are authorized by Federal or state law, we would not interfere with these important national security activities.

Under the final part of this proposal, we would permit covered entities that uncover evidence of health care fraud to disclose the protected health information that evidences such fraud to law enforcement officials without receiving a request from such officials. This provision would permit covered entities to make certain disclosures to law enforcement officials on their own

initiative if the information disclosed constitutes evidence of criminal conduct that arises out of and is directly related to (i) the receipt of health care or payment for health care (including a fraudulent claim for health care) or (ii) qualification for or receipt of benefits, payments or services based on a fraudulent statement or material misrepresentation of the health of a patient. Similarly, we would permit covered entities on their own initiative to disclose to law enforcement officials protected health information that the covered entity believes in good faith constitutes evidence of criminal conduct that either occurred on the covered entity's premises or was witnessed by an employee (or other workforce member) of the covered entity. In such situations, covered entities should be permitted to take appropriate steps to protect the integrity and safety of their operations or to assure that the such criminal conduct is properly prosecuted.

To be protected by this provision, the covered entity would have to have good faith belief that the disclosed protected health information was evidence of such conduct. If the covered entity disclosed protected health information in good faith but was wrong in its belief that the information evidenced a legal violation, the covered entity would not be subject to sanction under this regulation. We would not require the covered entity to accurately predict the outcome of a criminal investigation.

There also are situations where law enforcement officials would need access to information for emergency circumstances. In those cases, the disclosure could be made under § 164.510(k), ''Disclosure in emergency circumstances.''

Pursuant to § 164.518(c), covered entities would have an obligation to verify the identity of the person seeking disclosure of protected health information and the legal authority behind the request. As described in section II.H.3. of this preamble, we would permit covered entities to rely on a badge or similar identification to confirm that the request for protected health information is being made by a law enforcement official. If the request is not made in person, we would permit the covered entity to rely on official letter head or similar proof.

Where the covered entity must verify that lawful process has been obtained, § 164.518(c) would require the covered entity to review the document evidencing the order. The covered entity could not disclose more information than was authorized in the document.

Because the regulation applies to covered entities, and not to the law enforcement officials seeking the protected health information, the covered entity would not be in a position to determine with any certainty whether the underlying requirements for the process have been met. For instance, it may be difficult for the covered entity to determine whether the three-part test has been met for an administrative request. In light of this difficulty facing covered entities, the proposed rule would include a good faith provision. Under that provision, covered entities would not be liable under the rule for disclosure of protected health information to a law enforcement official where the covered entity or its business partners acted in a good faith belief that the disclosure was permitted under this title. We solicit comment on the extent to which this good faith provision would make the proposed rule less burdensome on covered entities and law enforcement officials. We also solicit comment on the extent to which the provision could undermine the effectiveness of the provision.

For requests for the conduct of intelligence activities or for protective services, covered entities would be required to verify the identity of the person or entity requesting the information, through a badge or other identification, or official letter head, as just described. If such verification of identity is obtained, covered entities would be permitted to reasonably rely on the representations of such persons that the request is for lawful national security or protective service activities and is authorized by law. Similarly, to disclose limited identifying information, covered entities would be required to obtain verification that the request comes from a law enforcement official, and would be permitted to reasonably rely on such official's representation that the information is needed for the purpose of identifying a suspect, fugitive, material witness, or missing person and is authorized by law.

iii. *Additional considerations.* This section 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, although it is not intended to create a basis for appealing to federal court concerning a request by state law enforcement officials. Each covered entity would continue to have available legal procedures applicable in the appropriate jurisdiction to contest such requests where warranted. This proposed rule would 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 for law enforcement purposes where other sections of the rule permit such disclosure, e.g., as permitted by § 164.510 under emergency circumstances, for oversight or public health activities, to coroners or medical examiners, and in other circumstances permitted by the rule.

In obtaining protected health information, law enforcement officials would have to comply with whatever other law was applicable. In certain circumstances, while this subsection could authorize a covered entity to disclose protected health information to law enforcement officials, there could be additional applicable statutes 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 proposed §§ 160.201 through 160.204. For example, if State law would permit disclosure only after compulsory process with court review, a provider or payer would not be allowed to disclose information to state law enforcement officials unless the officials had 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, would continue to be governed by those provisions.

In some instances, disclosure of protected health information to law enforcement officials would 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 prescription controlled substances). Disclosure of protected health information under such other mandatory law would be permitted under proposed § 164.510(n).

In developing our proposal, we considered permitting covered entities to disclose protected health information pursuant to any request made by a law enforcement official, rather than requiring some form of legal process or narrowly defined other circumstances. We rejected this option because we believe that in most instances some form of review should be required. Individuals' expectation of privacy with respect to their health information is sufficiently strong to require some form of process prior to disclosure to the

government. At the same time, we recognize that the public interest would not be served by requiring such formal process in every instance. Under our proposal, therefore, law enforcement could obtain certain identifying information in order to identify suspects and witnesses, and could obtain information for national security or protective services activities or in emergency circumstances. Similarly, we would not require process before a law enforcement official could obtain information about the victim of a crime, where the information is necessary as the basis for immediate action. In addition, in seeking an appropriate balance between public safety and individuals' expectation of privacy, we are proposing that covered entities not be subject to enforcement under this regulation if they disclose protected health information to law enforcement officials in a good faith belief that the disclosure was permitted under this title.

We solicit comment on what additional steps, if any, are appropriate for allowing law enforcement access to protected health information. We are interested in comments concerning situations where needed access to protected health information would not be available under these or other provisions of this proposed rule. We also seek comment on specific privacy or other concerns that would apply if the final regulation included provision for law enforcement access to protected health information without requiring a judicial order, grand jury subpoena, or administrative request, under such additional defined circumstances.

In some of these instances, release of protected health information would be authorized under the proposed regulation pursuant to provisions for patient consent, health oversight, emergency circumstances, or under mandatory reporting laws for gunshot wounds or abuse cases. We are interested in comments concerning situations where needed access to protected health information would not be available under these or other provisions of this proposed rule. We also seek comment on specific privacy or other concerns that would apply if the final regulation included provision for law enforcement access to protected health information without requiring a judicial order, grand jury subpoena, or administrative request, under such additional defined circumstances.

Our proposal with respect to law enforcement has been shaped by 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 proposed 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 as in the proposed regulation. 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 court of oversight activities. These limitations on our regulatory authority provide additional reason to support comprehensive medical privacy legislation.

6. Uses and Disclosures for Governmental Health Data Systems (§ 164.510(g))

[*Please label comments about this section with the subject: ''Governmental health data systems''*]

In § 164.510(g), we propose to permit covered entities to disclose protected health information for inclusion in State or other governmental health data systems without individual authorization when such disclosures are authorized by State or other law in support of policy, planning, regulatory or management functions.

a. *Importance of Governmental health data systems and the need for protected health information.* Governmental agencies collect and analyze individually identifiable health information as part of their efforts to improve public policies and program management, improve health care and reduce costs, and improve information available for consumer choices. Governments use the information to analyze health care outcomes, quality, costs and patterns of utilization, effects of public policies, changes in the health care delivery system, and related trends. These important purposes are related to public health, research and oversight (although the information in State or other governmental data systems usually is not collected specifically to audit or evaluate health care providers or for public health surveillance). The data are an important resource that can be used for multiple public policy evaluations.

The collection of health information by governmental health data systems often occurs without specification of the particular analyses that could be conducted with the information. These governmental data collection programs frequently call for reporting of information for all individuals treated or released by specified classes of providers. For example, many States request and receive from hospitals records containing individual diagnosis and treatment data for all discharges from their facilities. State hospital discharge data have been used to compare treatment practices and costs between hospitals, to evaluate implications for funding of health care, as well as to provide hospital ''report cards'' to consumers. As part of its general evaluation activities, the DOD maintains a very large database, called the Comprehensive Clinical Evaluation Program, involving military personnel who have reported illnesses possibly arising from service during the Gulf War.

b. *Proposed requirements.* We propose to permit covered entities to disclose protected health information for inclusion in State or other governmental health data systems when such disclosure is authorized by law for analysis in support of policy, planning, regulatory, and management functions. The recipient of the information must be a government agency (or privacy entity acting on behalf of a government agency). Where the covered entity is itself a government agency that collects health data for analysis in support of policy, planning, regulatory, or management functions, it would be permitted to use protected health information in all cases in which it is permitted to disclose such information for government health data systems under this section.

We believe that Congress intended to permit States, Tribes, territories, and other governmental agencies to operate health data collection systems for analyzing and improving the health care system. In section 1178(c), ''State regulatory reporting,'' HIPAA provides that it is not limiting the ability of a State to require a health plan to report, or to provide access to, information for a variety of oversight activities, as well as for ''program monitoring and evaluation.'' We also believe that the considerations Congress applied to State capacities to collect data would apply to similar data collection efforts by other levels of government, such as those undertaken by Tribes, territories and federal agencies. Therefore, we considered two questions regarding governmental health data systems; first,

which entities could make such disclosures; and second, what type of legal authority would be necessary for the disclosure to be permitted.

We considered whether to allow disclosure by all covered entities to governmental data collection systems or to limit permitted disclosures to those made by health plans, as specified in the regulatory reporting provision of HIPAA. While this provision only mentions data collected from health plans, the conference agreement notes that laws regarding ''State reporting on health care delivery or costs, or for other purposes'' should not be preempted by this rule. States would be likely to require sources of information other than health plans, such as health care providers or clearinghouses, in order to examine health care delivery or costs. Therefore, we do not believe it is appropriate to restrict States' or other governmental agencies' ability to obtain such data. This viewpoint is consistent with the Recommendations, which would permit this disclosure of protected health information by all covered entities.

We also asked what type of law would be required to permit disclosure without individual authorization to governmental health data systems. We considered requiring a specific statute or regulation that requires the collection of protected health information for a specified purpose. A law that explicitly addresses the conditions under which protected health information is collected would provide individuals and covered entities with a better understanding of how and why the information is to be collected and used.

We understand, however, that explicit authority to collect information is not always included in relevant law. Governmental agencies may collect health data using a broad public health or regulatory authority in statute or regulation. For example, a law may call on a State agency to report on health care costs, without providing specific authority for the agency to collect the health care cost data they need do so. Consequently, the agency may use its general operating authority to request health care providers to release the information. We recognize that many governmental agencies rely on broad legal authority for their activities and do not intend this proposed rule to hamper those efforts.

Under § 164.518(c), covered entities would have an obligation to verify the identity of the person requesting protected health information, and the legal authority behind the request before the disclosure would be permitted under this subsection. Preamble section II.G.3. describes these requirements in more detail.

7. Disclosure of Directory Information (§ 164.510(h))

[*Please label comments about this section with the subject: ''Directory information''*]

In § 164.510(h), we propose to permit covered entities to disclose information that could reveal protected health information about an individual for purposes of a facility patient directory, if the individual has indicated consent to such disclosures, or if the individual who is incapacitated had not previously expressed a preference in this regard and a covered entity determines that including such information in the directory would be consistent with good medical practice. Directory information could include only the person's name, location in the institution, and general condition.

a. *Importance of directory information and need for protected health information.* When individuals enter inpatient facilities, they are not always able to contact people who may need to know their whereabouts, want to visit them, or want to send them flowers or some other expression of concern. Today, facilities typically operate patient directories, allowing confirmation of a person's presence in a facility, providing the room number for visits and deliveries, and sometime providing general information on the patient's condition. These services cannot be performed without disclosing protected health information. Since most patients find this a welcome convenience, we believe it would be important to allow these practices to continue. However, not everyone may appreciate this service. We are proposing to accommodate the wishes of such people, where possible.

b. *Proposed requirements.* In § 164.510(h), we would require covered entities to ask individuals whether they wish to be included in the entity's directory. For individuals who are incapacitated or otherwise unable to communicate their wishes and who have not previously expressed a preference, the decision would be left to the discretion of the covered entity, consistent with good medical practice. We note that legal representatives could make such decisions on behalf of persons who are incapacitated or otherwise unable to communicate their wishes, consistent with State or other law, since they would stand as the ''individual.'' In the absence of a legal representative or prior expression of a preference by the individual, the decision would be left to the discretion of the covered entity, consistent with good medical practice.

i. *Individuals capable of making decisions.*

For individuals who are not incapacitated, this rule would require the covered entity to ask whether information about the individual's presence in the facility, room number and general condition can be included in the general patient directory. When individuals are capable of making such a determination, their wishes should be respected.

We considered whether also to require covered entities to allow an individual to specify that information can be provided to specific persons but not others. For example, someone may feel that it is acceptable to release information to family members but not to friends. While we would like to respect individuals' wishes to the greatest extent possible, we are concerned about placing on covered entities the burden of verifying the identify of a person requesting directory information. We are therefore not including this additional requirement, but are requesting comments on current practices and how such requests might be accommodated.

We would not require a formal individual authorization pursuant to § 164.508. A verbal or other informal inquiry and agreement would be sufficient. We require only that individuals be given the choice.

ii. *Incapacitated individuals.*

If an individual is not able to make determinations as to whether location or status information should be released to family and friends, and had not in the past expressed a preference in this regard, we would leave the decision as to whether to include the individual in a directory to the discretion of the covered entity. Often individuals are unconscious or otherwise unable due to a medical condition to communicate their wishes to the entity and no representative is available to act for them. In these cases, we encourage the covered entity to take into consideration a number of factors when deciding whether or not to include such an individual in the directory:

- Could disclosing that an individual is in the facility reasonably cause danger of harm to the individual? For example, if a person is unconscious and receiving treatment for injuries resulting from physical abuse from an unknown source, an entity may determine that revealing that the individual is in the facility could give the attacker enough information to seek out the individual and repeat the abuse.

• Could disclosing the location within the facility of the patient give information about the condition of the patient? If a patient's room number would reveal the nature of the medical condition, the entity may decide that it is inappropriate to give that information. For example, if one floor of a hospital has been specifically designated as the psychiatric floor, simply saying that a patient is located on that floor discloses some information about the condition of the individual.

• Is it necessary or appropriate to give the status of a patient to family or friends? Covered entities often need information from family or friends for the treatment of an incapacitated individual. For example, if a patient is unconscious, family or friends may be able to give valuable information that will assist the care giver in making urgent decisions. Family members or friends may be able to give information on drugs or medications that the individual has been taking. On the other hand, it may be that revealing the status of an individual gives more information than the individual would have disclosed if they could make the determination themselves.

• If an individual had, prior to becoming incapacitated, expressed a desire not to be included in such a directory and the covered entity learns of that statement of preference, the covered entity would be required to act in accordance with the stated preference.

Individuals who enter a facility incapacitated and then improve to the point of being able to make their own determinations should be asked within a reasonable time period for permission to include information in the facility's directory.

When the condition of an individual who has opted not to allow protected health information to be included in the facility's directory deteriorates, and the individual is no longer capable of making disclosure decisions, the covered entity would be required to abide by the individual's initial decision. However, such a decision should not prevent a provider from contacting the family if such contact is required for good medical practice. A provider could need information from the family to treat a newly incapacitated person. If good medical practice would include contacting family or friends, the individual's initial request should not prohibit such contact. But the covered entity would still be prohibited from including information about the individual in its directory.

8. Disclosure for Banking and Payment Processes (§ 164.510(i))

[*Please label comments about this section with the subject: ''Banking and payment processes''*]

In § 164.510(i), we propose to allow covered entities to disclose protected health information to financial institutions, or entities acting for financial institutions, if necessary for processing payments for health care and health care premiums.

a. *Importance of financial transactions and the need for protected health information.* Checks that individuals use to pay for health care typically include the names of providers or provider groups that could implicitly identify the medical condition for which treatment was rendered. Similarly, a credit card transaction will also reveal the identify of the provider and thus potentially the nature of the medical condition involved. While such information would constitute protected health information under this rule, there is no practical way of concealing this information when the provider deposits the check or claims credit card payment. Failure to allow this kind of disclosure of protected health information would impede the efficient operations of the health care system.

b. *Proposed requirements.* We propose that covered entities be permitted to disclose protected health information to financial institutions for the specific purposes listed in the section. The permissible purposes are those identified in the statute, and the regulatory text would copy the statutory list of allowable uses.

Under section 1179 of the Act, activities of financial institutions are exempt from HIPAA's Administrative Simplification requirements to the extent that those activities constitute ''authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments'' for health care or health plan premiums. This section of the statute states that financial institutions can use or disclose protected health information for these purposes. We read this part of the statute as indicating that Congress intended that this regulation not impede the efficient processing of these transactions, and accordingly are allowing covered entities to disclose protected health information to financial institutions for the purposes listed in section 1179 of the statute.

Proposed § 164.510(i) would not allow covered entities to include any diagnostic or treatment information in the data transmitted to financial institutions. Such information is never necessary to process a payment transaction. We believe 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 payer 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 (i.e., credit card expiration date); and (6) the individual's signature. At this time, we are not proposing to include in the regulation an exclusive list of information that could be lawfully disclosed for this purpose. We are, however, soliciting comment on whether more elements would be necessary for these banking and payment transactions and on whether including a specific list of the protected health information that could be disclosed is an appropriate approach.

We understand that financial institutions may also provide covered entities that accept payment via credit card with software that, in addition to fields for information required to process the transaction, includes blank fields in which health plans or health care providers may enter any type of information regarding their patients, such as diagnostic and treatment information, or other information that the covered entity wished to track and analyze. Other financial institutions could provide services to covered entities that constitute ''health care operations'' as defined in proposed § 164.504.

We do not know whether and to what extent health plans and health care providers are using such software to record and track diagnostic and treatment and similar information. However, we recognize that the capability exists and that if a plan or provider engages in this practice, information not necessary for processing the payment transaction could be forwarded to financial institutions along with other information used to process payments. Disclosing such information to a financial institution (absent a business partner relationship) would violate the provisions of this rule.

We also understand that banks, in addition to offering traditional banking services, may be interested in offering additional services to covered entities such as claims management and billing support. Nothing in this regulation would prohibit banks from becoming the business partners of covered entities in accordance with and subject to the conditions of § 164.506(e). If a bank offers an integrated package of traditional banking services and health claims and billing services, it could do