BILLING CODE: 4153-01

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Parts 160 and 164

Rin: 0991-AB14

Standards for Privacy of Individually Identifiable Health Information

AGENCY: Office for Civil Rights, HHS.

ACTION: Proposed rule; modification.

SUMMARY: The Department of Health and Human Services (HHS) proposes to modify certain standards in the Rule entitled "Standards for Privacy of Individually Identifiable Health Information" (the "Privacy Rule"). The Privacy Rule implements the privacy requirements of the Administrative Simplification subtitle of the Health Insurance Portability and Accountability Act of 1996.

The purpose of this action is to propose changes that maintain strong protections for the privacy of individually identifiable health information while clarifying misinterpretations, addressing the unintended negative effects of the Privacy Rule on health care quality or access to health care, and relieving unintended administrative burden created by the Privacy Rule.

DATES: To assure consideration, written comments mailed to the Department as provided below must be postmarked no later than [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER], and written comments hand delivered to the Department and comments submitted electronically must be received as provided below, no later than 5 p.m. on [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Comments will be considered only if provided through any of the following means:

1. Mail written comments (1 original and, if possible, 3 copies and a floppy disk) to the following address: U.S. Department of Health and Human Services, Office for Civil Rights, Attention: Privacy 2, Hubert H. Humphrey Building, Room 425A, 200 Independence Avenue, SW, Washington, DC 20201.

2. Deliver written comments (1 original and, if possible, 3 copies and a floppy disk) to the following address: Attention: Privacy 2, Hubert H. Humphrey Building, Room 425A, 200 Independence Avenue, SW, Washington, DC 20201.

3. Submit electronic comments at the following website: http://www.hhs.gov/ocr/hipaa/.

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

FOR FURTHER INFORMATION CONTACT: Felicia Farmer, 1-866-OCR-PRIV (1-866-627-7748) or TTY 1-866-788-4989.

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. Comments should address only those sections of the Privacy Rule for which modifications are being proposed or for which comments are requested. Comments on other sections of the Privacy Rule will not be considered, except insofar as they pertain to the standards for which modifications are proposed or for which comments are requested. Each specific comment should specify the section of the Privacy Rule to which it pertains.

Written comments should include 1 original and, if possible, 3 copies and an electronic version of the comments on a 3 ½ inch DOS format floppy disk in HTML, ASCII text, or popular word processor format (Microsoft Word, Corel WordPerfect). All comments and content must be limited to the 8.5 inches wide by 11.0 inches high vertical (also referred to as "portrait") page orientation. Additionally, if identical/duplicate comment submissions are submitted both electronically at the specified web site and in paper form, the Department requests that each submission clearly indicate that it is a duplicate submission.

Because of staffing and resource limitations, the Department will not accept comments by telephone or facsimile (FAX) transmission. Any comments received through such media will be deleted or destroyed, as appropriate, and not be considered as public comments. The Department will accept electronic comments only as submitted through the web site identified in the ADDRESSES section above. No other form of electronic

mail will be accepted or considered as public comment. In addition, when mailing written comments, the public is encouraged to submit comments as early as possible due to potential delays in mail service.

Inspection of Public Comments: Comments that are timely received in proper form and at one of the addresses specified above will be available for public inspection by appointment as they are received, generally beginning approximately three weeks after publication of this document, at 200 Independence Avenue, SW, Washington, DC, on Monday through Friday of each week from 9 a.m. to 4 p.m. Appointments may be made by telephoning 1-866-OCR-PRIV (1-866-627-7748) or TTY 1-866-788-4989.

Copies: To order copies of the Federal Register containing this document, send your request to: New Orders, Superintendent of Documents, P.O. Box 371954, Pittsburgh, PA 15250-7954. Specify the date of the issue requested and enclose a check or money order payable to the Superintendent of Documents, or enclose your Visa or Master Card number and expiration date. Credit card orders can also be placed by calling the order desk at (202) 512-1800 (or toll-free at 1-866-512-1800) or by fax to (202) 512-2250. The cost for each copy is $10.00. Alternatively, you may 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 the OCR Privacy Web site at http://www.hhs.gov/ocr/hipaa/, 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. Statutory Background.

Congress recognized the importance of protecting the privacy of health information given the rapid evolution of health information systems in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, which became law on August 21, 1996. HIPAA's Administrative Simplification provisions, sections 261 through 264 of the statute, were designed to improve the efficiency and effectiveness of the health care system by facilitating the electronic exchange of information with respect to financial and administrative transactions carried out by health plans, health care clearinghouses, and health care providers who transmit information electronically in connection with such transactions. To implement these provisions, the statute directed HHS to adopt a suite of uniform, national standards for transactions, unique health identifiers, code sets for the data elements of the transactions, security of health information, and electronic signature.

At the same time, Congress recognized the challenges to the confidentiality of health information presented by the increasing complexity of the health care industry, and by advances in the health information systems technology and communications. Thus, the Administrative Simplification provisions of HIPAA authorized the Secretary to promulgate regulations on standards for the privacy of individually identifiable health information if Congress did not enact health care privacy legislation by August 21, 1999. HIPAA also required the Secretary of HHS to provide Congress with recommendations for protecting the confidentiality of health care information. The Secretary submitted such

recommendations to Congress on September 11, 1997, but Congress was unable to act within its self-imposed deadline.

With respect to these regulations, HIPAA provided that the standards, implementation specifications, and requirements established by the Secretary not supersede any contrary State law that imposes more stringent privacy protections. Additionally, Congress required that HHS consult with the National Committee on Vital and Health Statistics, a Federal Advisory committee established pursuant to section 306(k) of the Public Health Service Act (42 U.S.C. 242k(k)), and the Attorney General in the development of HIPAA privacy standards.

After a set of standards is adopted by the Department, HIPAA provides HHS with authority to modify the standards as deemed appropriate, but not more frequently than once every 12 months. However, modifications are permitted during the first year after adoption of the standard if the changes are necessary to permit compliance with the standard. HIPAA also provides that compliance with modifications to standards or implementation specifications must be accomplished by a date designated by the Secretary, which may not be earlier than 180 days from the adoption of the modification.

B. Regulatory and Other Actions To Date

As Congress did not enact legislation regarding the privacy of individually identifiable health information prior to August 21, 1999, HHS published a proposed Rule setting forth such standards on November 3, 1999 (64 FR 59918). The Department received more than 52,000 public comments in response to the proposal. After reviewing

and considering the public comments, HHS issued a final Rule (65 FR 82462) on December 28, 2000, establishing "Standards for Privacy of Individually Identifiable Health Information" ("Privacy Rule").

In an era where consumers are increasingly concerned about the privacy of their personal information, the Privacy Rule creates for the first time national protections for the privacy of their most sensitive information - health information. Congress has passed other laws to protect consumer's personal information contained in bank, credit card, other financial records, and even video rentals. These health privacy protections are intended to provide consumers with similar assurances that their health information, including genetic information, will be properly protected. Under the Privacy Rule, health plans, health care clearinghouses, and certain health care providers must guard against misuse of individuals' identifiable health information and limit the sharing of such information, and consumers are afforded significant new rights to understand and control how their health information is used and disclosed.

After publication of the Privacy Rule, HHS received many inquiries and unsolicited comments through telephone calls, e-mails, letters, and other contacts about the impact and operation of the Privacy Rule on numerous sectors of the health care industry. Many of these commenters exhibited substantial confusion over how the Privacy Rule will operate; others expressed great concern over the complexity of the Privacy Rule. In response to these communications and to ensure that the provisions of the Privacy Rule would protect patients' privacy without creating unanticipated consequences that might harm patients' access to health care or quality of health care; the Secretary of HHS

requested comment on the Privacy Rule in March 2001 (66 FR 12738). After an expedited review of the comments by the Department, the Secretary decided that it was appropriate for the Privacy Rule to become effective on April 14, 2001, as scheduled (65 FR 12433). At the same time, the Secretary directed the Department immediately to begin the process of developing guidelines on how the Privacy Rule should be implemented and to clarify the impact of the Privacy Rule on health care activities. In addition, the Secretary charged the Department with proposing appropriate changes to the Privacy Rule during the next year to clarify the requirements and correct potential problems that could threaten access to, or quality of, health care. The comments received during the comment period, as well as other communications from the public and all sectors of the health care industry, including letters, testimony at public hearings, and meetings requested by these parties, have helped to inform the Department's efforts to develop proposed modifications and guidance on the Privacy Rule.

On July 6, 2001, the Department issued its first guidance to answer common questions and clarify certain of the Privacy Rule's provisions. In the guidance, the Department also committed to proposing modifications to the Privacy Rule to address problems arising from unintended effects of the Privacy Rule on health care delivery and access. The guidance is available on the HHS Office for Civil Rights (OCR) Privacy Web site at http://www.hhs.gov/ocr/hipaa/.

II. Overview of the Proposed Rule

As described above, through public comments, testimony at public hearings,

meetings at the request of industry and other stakeholders, as well as other communications, the Department learned of a number of concerns about the potential unintended effect certain provisions would have on health care delivery and access. In response to these concerns, and pursuant to HIPAA's provisions for modifications to the standards, the Department is proposing modifications to the Privacy Rule.

In addition, the National Committee for Vital and Health Statistics (NCVHS), Subcommittee on Privacy and Confidentiality, held public hearings on the implementation of the Privacy Rule on August 21-23, 2001, and January 24-25, 2002, and provided recommendations to the Department based on these hearings. The NCVHS serves as the statutory advisory body to the Secretary of HHS with respect to the development and implementation of the Rules required by the Administrative Simplification provisions of HIPAA, including the privacy standards. Through the hearings, the NCVHS specifically solicited public input on issues related to certain key standards in the Privacy Rule: consent, minimum necessary, marketing, fundraising, and research. The resultant public testimony and subsequent recommendations submitted to the Department by the NCVHS also served to inform the development of these proposed modifications.

Based on the information received through the various sources described above, the Department proposes to modify the following areas or provisions of the Privacy Rule: consent, including other provisions for uses and disclosures of protected health information for treatment, payment, and health care operations; notice of privacy practices for protected health information; minimum necessary uses and disclosures, and oral communications; business associates; uses and disclosures for marketing; parents as the

personal representatives of unemancipated minors; uses and disclosures for research purposes; uses and disclosures of protected health information for which authorizations are required; and de-identification of protected health information. In addition to these key areas, the proposal includes changes to certain other provisions where necessary to clarify the Privacy Rule. The Department also includes in the proposed Rule a list of technical corrections intended as editorial or typographical corrections to the Privacy Rule.

The proposed modifications collectively are designed to ensure that protections for patient privacy are implemented in a manner that maximizes the effectiveness of such protections while not compromising either the availability or the quality of medical care. They reflect a continuing commitment on the part of the Department to strong privacy protections for medical records and the belief that privacy is most effectively protected by requirements that are not exceptionally difficult to implement. If there are any ways in which privacy protections are unduly compromised by these modifications, the Department welcomes comments and suggestions for alternative ways effectively to protect patient privacy without adversely affecting access to, or the quality of, health care.

Given that the compliance date of the Privacy Rule for most covered entities is April 14, 2003, and statutory requirements to ensure that affected parties have sufficient time to come into compliance require any revisions to become effective by October 13, 2002, the Department is soliciting public comment on these proposed modifications for only 30 days. As stated above, the modifications address public concerns already communicated to the Department through a wide variety of sources since publication of

the Privacy Rule in December 2000. For these reasons, the Department believes that 30 days should be sufficient for the public to state its views fully to the Department on the proposed modifications to the Privacy Rule.

III. Description of Proposed Modifications

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

1. Consent

Treatment and payment for health care are core functions of the health care industry, and uses and disclosures of individually identifiable health information for such purposes are critical to the effective operation of the health care system. Health care providers and health plans must also use individually identifiable health information for certain health care operations, such as administrative, financial, and legal activities, to run their businesses, and to support the essential health care functions of treatment and payment. Equally important are health care operations designed to maintain and improve the quality of health care. In developing the Privacy Rule, the Department considered the privacy implications of uses and disclosures for treatment, payment, and health care operations in connection with the need for these activities to continue. In balancing the need for these activities and the privacy interests involved in using and disclosing protected health information for these purposes, the Department considered the fact that many individuals expect that their health information will be used and disclosed as necessary to treat them, bill for treatment, and, to some extent, operate the covered entity's health care business. Due to individual expectations with respect to the use or

disclosure of information for such activities and so as not to interfere with an individual's access to quality health care or efficient payment for such health care, the Department's goal is to permit these activities to occur with little or no restriction.

Consistent with this view, the Privacy Rule generally provides covered entities with permission to use and disclose protected health information as necessary for treatment, payment, and health care operations. For certain health care providers that have a direct treatment relationship with individuals, such as many physicians, hospitals, and pharmacies, the Privacy Rule requires such providers to obtain an individual's written consent prior to using or disclosing protected health information for these purposes.

To implement the consent standard, the Privacy Rule requires a covered health care provider with a direct treatment relationship with the individual to obtain a single, one-time, general permission from the individual prior to using or disclosing protected health information about him or her for treatment, payment, and health care operations. An individual may revoke his or her consent at any time, except to the extent that the covered entity has taken action in reliance on the consent. The Privacy Rule contains exceptions to the consent requirements, under which a provider may use or disclose protected health information without prior consent when there is an emergency treatment situation, when a provider is required by law to treat the individual, or when there are substantial communication barriers. Additionally, because the Department realizes that a health care provider cannot treat a patient without being able to use and disclose his or her protected health information for treatment purposes, the Privacy Rule permits a covered health care provider to refuse to treat a patient who refuses to provide consent. Finally,

the Privacy Rule permits other covered entities to voluntarily obtain consent, in accordance with these consent provisions.

The consent requirement for health care providers with direct treatment relationships was a significant change from the Department's initial proposal published in November 1999. At that time, the Department proposed to permit all covered entities to use and disclose protected health information to carry out treatment, payment, and health care operations without any requirement that the covered entities obtain an individual's consent for such uses and disclosures, subject to a few limited exceptions. Further, the Department had proposed to prohibit covered entities from obtaining an individual's consent for uses and disclosures of protected health information for these purposes, unless required by other applicable law. Instead, the Department relied on the principle of fair notice, coupled with regulatory limits on the use and disclosure of health information, to balance the individual's privacy interests against the need not to impede the delivery of quality health care. Providing individuals with fair notice about the information practices and responsibilities of their plans and providers, and their rights with respect to information about them, is a privacy principle as important as the principle of consent. Indeed, consents often provide individuals with little actual control over information. When an individual is required to sign a blanket consent at the point of treatment as a condition of treatment or payment, that consent is often not voluntary. Instead, therefore, the Department proposed to require most covered entities to create and provide to individuals a notice describing all of the entity's information practices, including their practices with respect to uses and disclosures of protected health information to carry out

treatment, payment, and health care operations.

The Department received a strong public response opposing this proposal. Health care providers and patients argued that consent provides individuals with a sense of control over how their information will be used and disclosed, is a current practice of many health care providers, and is expected by patients. Providers explained that they would face an ethical conflict from a prohibition on obtaining consent. The consent requirement for direct treatment providers was a direct response to these comments.

Public Comments

The Department received many comments in March 2001, as well as recommendations from the NCVHS based on public testimony, about the consent provisions in the Privacy Rule. There were some proponents of consent that urged the Department to retain, expand, or strengthen the consent provisions. There were also many opponents of consent that raised a number of issues and serious concerns that the consent requirements will impede access to, and the delivery of, quality health care. Most significantly, many covered entities described an array of circumstances when they need to use or disclose protected health information for treatment, payment, or health care operations purposes prior to the initial face-to-face contact with the patient, and therefore, prior to obtaining consent.

Consistent with the comments that the Department received after the initial notice of proposed rulemaking (NPRM), proponents of the consent requirement argued that consent is integral to providing individuals the opportunity to be active participants in their

own health care and can bolster patient trust in providers. One of the most significant values that proponents placed on consent was that it defines an "initial moment" when patients can focus on information practices and raise questions about privacy concerns. Some proponents recommended that the consent requirement be extended to health plans because these entities may not have the same duty and legal obligation as health care providers to maintain confidentiality.

Others urged the Department to strengthen consent by eliminating the ability of providers to condition treatment on the receipt of consent. There were also some commenters that thought that consent should be required more frequently. They claimed that the consent provisions will be ineffective to provide individuals with control over how their information will be used or disclosed because it is general and only must be obtained one time. They argued that an individual may have differing degrees of concern about the privacy of health information, depending on the nature of the information raised in the particular encounter with the provider, and that an initial, one-time consent cannot account for such variation.

At the same time, most covered entities were concerned about significant practical problems that resulted from the consent requirements in the Privacy Rule. Commenters raised numerous examples of obstacles that the prior consent provisions will pose to timely access to health care. Health care providers commented that they often use health information about an individual for necessary treatment, payment, and health care operations activities prior to the first face-to-face contact with the individual. Under the Privacy Rule, these routine and often essential activities are not permitted unless the

provider first obtains consent from the individual. Although the consent only needs to be obtained one time, there may be problems for new patients who have not yet provided consent, for existing patients who have not yet provided consent after the compliance date of the Privacy Rule, for patients who have revoked consent, and for patients who may have provided consent, but the provider cannot find such documentation.

These concerns were primarily raised by pharmacists and pharmacies, but the same issue exists in any referral or new patient situation. Pharmacists informed us that they typically use individually identifiable health information, received from a physician, to fill a prescription, search for potential drug interactions, and determine eligibility and obtain authorization for payment, before the individual arrives at the pharmacy to pick up the prescription. The consent requirement would delay such activity for any first-time customers and for many more customers immediately following the compliance date of the Privacy Rule. Tracking consents in large, multi-state pharmacy chains can result in delays as well. At best, an individual will experience significant delays in obtaining his or her prescription if a pharmacist cannot fill the prescription until the individual is present to sign a consent. Even greater delays may be experienced by individuals too ill to pick up their own prescriptions. Although the Privacy Rule permits a friend or neighbor to pick up the prescription, that person may not have the legal authority to sign a consent on the individual's behalf. Thus, a number of trips back and forth to the pharmacy may be needed to obtain the prior consent. This problem is greatly magnified in rural areas, where persons may travel much longer distances to see health care providers, including pharmacists.

Similarly, a hospital receives information about a patient from a referring physician and routinely uses this information to schedule and prepare for procedures before the individual presents at the hospital for such procedure. The Privacy Rule's requirement that a covered entity obtain an individual's consent prior to using or disclosing their information is an impediment to these activities and could require an individual to make an additional trip to the hospital simply to provide consent. The Department did not intend that the Privacy Rule interfere with such activities.

Commenters also raised concerns that providers who do not provide treatment in person may be unable to provide care because they are unable to obtain prior written consent to use protected health information at the first service delivery. This was a special concern with respect to providers who care for individuals over the telephone. For example, providers who cover for other providers during non-business hours or providers who had not yet had the opportunity to obtain a patient's consent were concerned that they would not be able to respond to telephone calls from individuals in need of treatment because they were not able to obtain consent over the telephone. Nurses who staff telephone centers that provide health care assessment and advice, but who never see patients, had similar concerns.

Other concerns related to treatment were expressed about the limitations of the exceptions to the consent requirement in the Privacy Rule. For example, emergency medical providers were unclear as to whether all activities in which they engage qualify for the emergency treatment exception to the consent requirement. As a result of this confusion, they were concerned that, if a situation was urgent, they would have to try to

obtain consent to comply with the Privacy Rule even if that would be inconsistent with current practice of emergency medicine. These providers also were concerned about the requirement that a provider must attempt to obtain consent as soon as reasonably practicable after an emergency. Emergency medical providers explained that they typically do not have ongoing relationships with individuals and that the requirement to attempt to obtain consent after the emergency would require significant efforts and administrative burden on their part, and would be viewed as harassment by individuals.

Providers who do not provide emergency care and who are not likely meet one of the consent exceptions were concerned that they may be put in the untenable position of having to decide whether to withhold treatment when an individual does not provide consent or proceed to use information to treat the individual in violation of the consent requirements.

Covered entities were also concerned that the difficultly in tracking consents may hamper treatment. The Privacy Rule permits an individual to revoke his or her consent. Large institutional providers claimed that, since tracking of patient consents and revocations would be very difficult and expensive, in practice, they would need to obtain consent for each patient encounter, rather than just one-time as allowed by the Privacy Rule. Covered entities were concerned that, if an individual revokes consent, they would have to eliminate all protected health information about that individual from their systems in order to ensure that it was not used inadvertently for routine health care operations purposes, which would hinder their quality improvement activities and other health care operations. Additionally, testimony before the NCVHS revealed a concern that the ability

of a patient to revoke consent might prevent health care providers from accessing protected health information that is critical for the treatment of an individual in an emergency treatment situation where a new consent is not obtained.

The Department also heard many concerns about the transition provisions related to the use and disclosure of protected health information for treatment, payment, or health care operations. The Privacy Rule permits covered health care providers that are required to obtain consent for treatment, payment, or health care operations to continue, after the compliance date of the Privacy Rule, to use and disclose protected health information they created or received prior to the compliance date of the Privacy Rule for these purposes if they have obtained consent, authorization, or other express legal permission to use or disclose such information for any of these purposes, even if such permission does not meet the consent requirements under the Privacy Rule. Many providers informed the Department that they currently were not required to obtain consent for these purposes, that these transition provisions would result in significant operational problems, and the inability to access health records would have an adverse effect on quality activities.

Concerns also were raised regarding the exception to the consent requirement for cases where a provider is required by law to treat an individual. For example, providers that are required by law to treat were concerned about the mixed messages to patients and interference with the physician-patient relationship that would result when they are required to ask for consent to use or disclose protected health information for treatment, payment, or health care operations, but if the patient says "no," they are permitted to use or disclose the information for such purposes anyway.

There also was confusion about the interaction of the consent provisions and the provisions regarding parents and minors. Testimony received by the NCVHS indicated uncertainty as to the validity of a consent signed by a parent for his or her minor child once the child reaches the age of majority. The NCVHS requested clarification regarding whether a child must sign a new consent upon reaching the age of majority.

The NCVHS hearings and recommendations focused on practical implementation issues, including the unintended consequences of the consent provisions, but did not address whether the Privacy Rule should or should not require consent. The NCVHS generally recommended that the Department consider circumstances in which protected health information could be used and disclosed without an individual's prior written consent and modify the Privacy Rule accordingly. The Committee specifically recommended that the Privacy Rule should be amended to include provisions for allowing covered entities to use and disclose protected health information prior to the initial face-to-face contact with an individual.

Proposed Modifications

The Department is concerned by the multitude of comments and examples demonstrating that the consent requirements result in unintended consequences that impede the provision of health care in many critical circumstances and that other such unintended consequences may exist which have yet to be brought to its attention. However, the Department understands that the opportunity to discuss privacy practices and concerns is an important component of privacy, and that the confidential relationship

between a patient and a health care provider includes the patient's ability to be involved in discussions and decisions related to the use and disclosure of any protected health information about him or her.

Accordingly, the Department proposes an approach that protects privacy interests by affording patients the opportunity to engage in important discussions regarding the use and disclosure of their health information, while allowing activities that are essential to provide access to quality health care to occur unimpeded. Specifically, the Department proposes to make optional the obtaining of consent to use and disclose protected health information for treatment, payment, or health care operations on the part of all covered entities, including providers with direct treatment relationships. Under this proposal, health care providers with direct treatment relationships with individuals would no longer be required to obtain an individual's consent prior to using and disclosing information about him or her for treatment, payment, and health care operations. They, like other covered entities, would have regulatory permission for such uses and disclosures.

In order to preserve flexibility and the valuable aspects of the consent requirement, the Department proposes changes that would: (1) permit all covered entities to obtain consent if they choose, (2) strengthen the notice requirements to preserve the opportunity for individuals to discuss privacy practices and concerns with providers, and (3) enhance the flexibility of the consent process for those covered entities that choose to obtain consent. See section III.B. of the preamble below for the related discussion of proposed modifications to the Privacy Rule's notice requirements.

Other individual rights would not be affected by this proposal. Although covered

entities would not be required to obtain an individual's consent, any uses or disclosures of protected health information for treatment, payment, or health care operations would still need to be consistent with the covered entity's notice of privacy practices. Also, the removal of the consent requirement only applies to consent for treatment, payment, and health care operations; it does not alter the requirement to obtain an authorization under § 164.508 for uses and disclosures of protected health information not otherwise permitted by the Privacy Rule. The functions of treatment, payment, and health care operations were all given carefully limited definitions in the Privacy Rule, and the Department intends to enforce strictly the requirement for obtaining an individual's authorization, in accordance with § 164.508, for uses and disclosure of protected health information for other purposes not otherwise permitted or required by the Privacy Rule. Furthermore, individuals would retain the right to request restrictions, in accordance with § 164.522(a).

Although consent for use and disclosure of protected health information for treatment, payment, and health care operations would no longer be mandated, the Department is proposing to allow covered entities to have a consent process if they wish to do so. The Department heard from some commenters that obtaining consent was an integral part of the ethical and other practice standards for many health care professionals. The Department, therefore, would not prohibit covered entities from obtaining consent.

Under this proposal, a consent could apply only to uses and disclosures that are otherwise permitted by the Privacy Rule. A consent obtained through this voluntary process would not be sufficient to permit a use or disclosure which, under the Privacy Rule, requires an authorization or is otherwise expressly conditioned. For example, a

consent could not be obtained in lieu of an authorization or a waiver of authorization by an IRB or Privacy Board to disclose protected health information for research purposes.

The Department proposes to allow covered entities that choose to have a consent process complete discretion in designing this process. The comments have informed the Department that one consent process and one set of principles will likely be unworkable. As a result, these proposed standards would leave complete flexibility to each covered entity. Covered entities that chose to obtain consent could rely on industry practices to design a voluntary consent process that works best for their practice area and consumers.

To effectuate these changes to the consent standard, the Department proposes to replace the consent provisions in § 164.506 with a new provision at § 164.506(a) that would provide regulatory permission for covered entities to use or disclose protected health information for treatment, payment, and health care operations, and a new provision at § 164.506(b) that would allow covered entities to obtain consent if they choose to, and make clear that such consent may not permit a use or disclosure of protected health information not otherwise permitted or required by the Privacy Rule. Additionally, the Department proposes a number of conforming modifications throughout the Privacy Rule to accommodate the proposed approach. The most substantive corresponding changes are proposed at §§ 164.502 and 164.532. Section 164.502(a)(1) provides a list of the permissible uses and disclosures of protected health information, and refers to the corresponding section of the Privacy Rule for the detailed requirements. The Department collapses the provisions at §§ 164.502(a)(1)(ii) and (iii) that address uses and disclosures of protected health information for treatment, payment, and health care operations and

modifies the language to eliminate the consent requirement for these purposes.

Section 164.532 consists of the transition provisions. In § 164.532, the Department deletes references to § 164.506 and to consent, authorization, or other express legal permission obtained for uses and disclosures of protected health information for treatment, payment, and health care operations prior to the compliance date of the Privacy Rule. The proposal to permit a covered entity to use or disclose protected health information for these purposes without consent or authorization would apply to any protected health information held by a covered entity whether created or received before or after the compliance date. Therefore, transition provisions would not be necessary.

The Department also proposes conforming changes to the definition of "more stringent" in § 160.202, § 164.500(b)(1)(v), §§ 164.508(a)(2)(i) and (b)(3)(i), the introductory text of §§ 164.510 and 164.512, the title of § 164.512, and § 164.520(b)(1)(ii)(B) to reflect that consent is no longer required.

2. Disclosures for treatment, payment, or health care operations of another entity

The Privacy Rule permits a covered entity to use and disclose protected health information for treatment, payment, or health care operations (subject to a consent in some cases). Uses and disclosures for treatment are broad because the definition of treatment incorporates the interaction among more than one entity; specifically, coordination and management of health care among health care providers or by a health care provider with a third party, consultations between health care providers, and referrals of a patient for health care from one health care provider to another. As a result, covered

entities are permitted to disclose protected health information for treatment regardless of to whom the disclosure is made, as well as to disclose protected health information for the treatment activities of another health care provider.

However, for payment and health care operations, the Privacy Rule generally limits a covered entity's uses and disclosures of protected health information to those that are necessary for its own payment and health care operations activities. This limitation is explicitly stated in the preamble discussions in the Privacy Rule of the definitions of "payment" and "health care operations." The Privacy Rule also provides that a covered entity must obtain authorization to disclose protected health information for the payment or health care operations of another entity. The Department intended these requirements to be consistent with individuals' privacy expectations. See §§ 164.506(a)(5) and 164.508(e).

Public Comments

A number of commenters raised specific concerns with the restriction that a covered entity is permitted to use and disclose protected health information only for its own payment and health care operations activities. These commenters presented a number of examples where such a restriction would impede the ability of certain covered entities to obtain reimbursement for health care, to conduct certain quality assurance or improvement activities, such as accreditation, or to monitor fraud and abuse.

With regard to payment, the Department received specific concerns about the difficultly that the Privacy Rule will place on certain providers trying to obtain information

needed for reimbursement for health care. Specifically, ambulance service providers explained that they normally receive the information they need to seek payment for treatment from the hospital emergency departments to which they transport their patients, since it is usually not possible at the time the service is rendered for the ambulance service provider to obtain such information directly from the individual. Nor is it practicable or feasible in all cases for the hospital to obtain the individual's authorization to provide payment information to the ambulance service provider after the fact. This disclosure of protected health information from the hospital to the ambulance service provider is not permitted under the Privacy Rule without an authorization from the patient because it is a disclosure by the hospital for the payment activities of the ambulance service provider.

In addition, commenters stated that physicians and other covered entities outsource their billing, claims, and reimbursement functions to accounts receivable management companies. These collectors often attempt to recover payments from a patient for care rendered by multiple health care providers. Commenters were concerned that the Privacy Rule will prevent these collectors, as business associates of multiple providers, from using a patient's demographic information received from one provider in order to facilitate collection for another provider's payment purposes.

With regard to health care operations, the Department also received comments about the difficultly that the Privacy Rule will place on health plans trying to obtain information needed for quality assessment activities. Health plans informed the Department that they need to obtain individually identifiable health information from health care providers for the plans' own quality-related activities, accreditation, and

performance measures, e.g., Health Plan Employer Data and Information Set (HEDIS). Commenters explained that the information provided to plans for payment purposes (e.g., claims or encounter information) may not be sufficient for quality assessment or accreditation purposes. Plans may receive even less information from their capitated providers.

The NCVHS also received specific public testimony with regard to this issue as part of public hearings held in August 2001. The NCVHS subsequently recommended to the Department that the Privacy Rule be amended to allow for uses and disclosures for quality-related activities among covered entities without individual written authorization.

Proposed Modifications

Based on concerns raised by comments, the Department proposes to modify § 164.506 to permit a covered entity to disclose protected health information for the payment activities of another covered entity or health care provider, and for certain health care operations of other covered entities. This proposal would broaden the uses and disclosures that are permitted as part of treatment, payment, and health care operations so as not to interfere inappropriately with access to quality and effective health care, while limiting this expansion in order continue to protect the privacy expectations of individuals. It would be a limited expansion of the information that is allowed to flow between entities, without an authorization, as part of treatment, payment, and certain health care operations.

The Department proposes the following. First, the Department explicitly includes

in § 164.506(c)(1) language stating that a covered entity may use or disclose protected health information for its own treatment, payment, or health care operations without prior consent or authorization.

Second, in § 164.506(c)(2), the Department includes language to clarify its intent that a covered entity may share protected health information for the treatment activities of another health care provider. For example, a primary care provider, who is a covered entity under the Privacy Rule, may send a copy of an individual's medical record to a specialist who needs the information to treat the same individual. No authorization would be required.

Third, with respect to payment, the Department proposes, in § 164.506(c)(3), to explicitly permit a covered entity to disclose protected health information to another covered entity or health care provider for the payment activities of that entity. The Department recognizes that not all health care providers who need protected health information to obtain payment are covered entities, and therefore, proposes to allow disclosures of protected health information to both covered and non-covered health care providers. The Department is unaware of any similar barrier with respect to plans that are not covered under the Privacy Rule to obtain the protected health information they need for payment purposes, but solicits comment on whether such barriers exist. Therefore, the Department proposes to limit disclosures under this provision to those health plans that are covered by the Privacy Rule.

Fourth, in § 164.506(c)(4), the Department proposes to permit a covered entity to disclose protected health information about an individual to another covered entity for

certain health care operations purposes of the covered entity that receives the information. The proposal would permit such disclosures only for the activities described in paragraphs (1) and (2) of the definition of "health care operations," as well as for health care fraud and abuse detection and compliance programs (as provided for in paragraph (4) of the definition of "health care operations"). The activities that fall into paragraphs (1) and (2) of the definition of "health care operations" include quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, case management, conducting training programs, and accreditation, certification, licensing, or credentialing activities. This provision is intended to allow information to flow from one covered entity to another for activities important to providing quality and effective health care.

The proposed expansion for permissible disclosures for health care operations without authorization is more limited than the permissible disclosures for treatment and payment in two ways. First, in contrast to treatment and payment, the proposal limits the types of health care operations that are covered by this expansion. The Department proposes this limitation because it recognizes that "health care operations" is a broad term and that individuals are less aware of the business-related activities that involve the use and disclosure of protected health information. In addition, many commenters and the NCVHS focused their comments on covered entities' needs to share protected health information for quality-related health care operations activities.

Second, in contrast to the treatment and payment provisions in this section, the proposal for disclosures of protected health information for health care operations of

another entity limits disclosures to other covered entities. By limiting disclosure for such purposes to entities that are required to comply with the Privacy Rule, the protected health information would continue to be protected. The Department believes that this would create the appropriate balance between meeting an individual's privacy expectations and meeting a covered entity's need for information for quality-related health care operations.

These proposed modifications to allow disclosures for health care operations of another entity are permitted only to the extent that each entity has, or has had, a relationship with the individual who is the subject of the information being requested. Where the relationship between the individual and the covered entity has ended, a disclosure of protected health information about the individual only would be allowed if related to the past relationship. The Department believes that this limitation is necessary in order to protect the privacy expectations of the individual. An individual should expect that two providers that are providing treatment to the individual, and the health plan that pays for the individual's health care, would have protected health information about the individual for health care operations purposes. However, an individual would not expect a health plan with which the individual has no relationship to be able to obtain identifiable information from his or her health care provider. Therefore, this proposed limitation would minimize the effect on privacy interests, while not interfering with covered entities' ability to continue to provide access to quality and effective health care.

These provisions do not eliminate a covered entity's responsibility to apply the Privacy Rule's minimum necessary provisions to both the disclosure of and request for information for payment and health care operations purposes. In addition, the Department

continues to strongly encourage the use of de-identified information wherever feasible.

The Department, however, is aware that the above proposal could pose barriers to disclosures for quality-related health care operations to plans and health care providers that are not covered entities, or to entities that do not have a relationship with the individual. For example, the proposal could be a problem for hospitals that share aggregated but identifiable information with other hospitals for health care operations purposes, when the recipient hospital does not have a relationship with the individual who is the subject of the information being disclosed. While the Department believes the proposed modification strikes the right balance between privacy expectations and covered entities' need for information for such purposes, the Department is considering permitting the disclosure of information that is not facially identifiable for quality-related purposes, subject to a data use or similar agreement. This would permit uses and disclosures for such purposes of a limited data set that does not include facially identifiable information, but in which certain identifiers remain. The Department is requesting comment on whether this approach would strike a proper balance. See section III.I of the preamble regarding de-identification of protected health information for a detailed discussion of this proposed approach.

Related to the above modifications, and in response to comments evidencing confusion on this matter, the Department proposes in § 164.506(c)(5) to make it clear that covered entities participating in an organized health care arrangement (OHCA) may share protected health information for the health care operations of the OHCA. The Privacy Rule allows legally separate covered entities that are integrated clinically or operationally

to be considered an OHCA for purposes of the Privacy Rule if protected health information must be shared among the covered entities for the joint management and operations of the arrangement. See the definition of "organized health care arrangement" in § 164.501. Additionally, the Privacy Rule, in the definition of "health care operations," permits the sharing of protected health information in an OHCA for such activities. The Department proposes to remove the language regarding OHCAs from the definition of "health care operations" as unnecessary because such language now would appear in § 164.506(c)(5).

In addition, the Department proposes a conforming change to delete the word "covered" in paragraph (1)(i) of the definition of "payment." This change would be necessary because the proposal would permit disclosures to non-covered providers for their payment activities.

B. Notice of Privacy Practices for Protected Health Information

The Privacy Rule requires most covered entities to provide individuals with adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights, and the covered entity's responsibilities, with respect to protected health information. See § 164.520. Content requirements for the notice are specified in the Privacy Rule. There are also specific requirements, which vary based on the type of covered entity, for providing such notice to individuals.

For example, a covered health care provider that has a direct treatment relationship

with an individual must provide the notice by the date of the first service delivery and, if such provider maintains a physical service delivery site, must post the notice in a clear and prominent location. In addition, whenever the notice is revised, the provider must make the notice available upon request. If the covered provider maintains a website, the notice must also be available electronically on the web site. If the first service delivery to an individual is electronic, the covered provider must furnish electronic notice automatically and contemporaneously in response to the individual's first request for service.

Proposed Modifications

In order to preserve some of the most important benefits of the consent requirement, the Department proposes to modify the notice requirements at § 164.520(c)(2) to require that a covered health care provider with a direct treatment relationship make a good faith effort to obtain an individual's written acknowledgment of receipt of the provider's notice of privacy practices. Other covered entities, such as health plans, would not be required to obtain this acknowledgment from individuals, but could do so if they chose.

The Department believes that promoting individuals' understanding of privacy practices is an essential component of providing notice to individuals. In addition, the Department believes it is just good business practice to provide individuals with fair notice about how their information will be used, disclosed, and protected. This proposal would strengthen the notice process by incorporating into the notice process the "initial moment" between a covered health care provider and an individual, where individuals may focus on

information practices and privacy rights and discuss any concerns related to the privacy of their protected health information. This express acknowledgment would also provide the opportunity for an individual to make a request for additional restrictions on the use or disclosure of his or her protected health information or for additional confidential treatment of communications, as permitted under § 164.522.

The Department intends the proposed notice acknowledgment requirement to be simple and not impose a significant burden on either the covered health care provider or the individual. First, the requirement for good faith efforts to obtain a written acknowledgment only applies to covered providers with direct treatment relationships. This is the same group of covered entities that would have been required to obtain consent under the Privacy Rule. The Department believes that these are the covered entities that have the most direct relationships with individuals, and therefore, the entities for which the requirement will provide the greatest privacy benefit to individuals with the least burden to covered entities.

Second, the Department designed the timing of the proposed good faith acknowledgment requirement to limit the burden on covered entities by generally making it consistent with the timing for notice distribution. Therefore, with one exception, a covered health care provider would be required to make good faith efforts to obtain a written acknowledgment of the notice at the time of first service delivery–the same time that the notice must be provided. The Department understands, however, that providing notice and obtaining an acknowledgment is not practicable during emergency treatment situations. In these situations, the Department proposes in § 164.520(c)(2) to delay the

requirement for provision of notice until reasonably practicable after the emergency treatment situation, and exempt health care providers from having to make a good faith effort to obtain the acknowledgment in emergency treatment situations.

Third, the proposal does not prescribe in detail the form the acknowledgment must take. Rather, the Department proposes to require only that the acknowledgment be in writing, and intends to allow each covered health care provider to choose the form and other details of the acknowledgment that are best suited to the entity's practices and that will not pose an impediment to the delivery of timely, quality health care. While the Department believes that requiring the individual's signature is preferable because an individual is likely to pay more attention or more carefully read a document that he or she signs, the proposal does not require an individual's signature on the notice. An acknowledgment under this proposed modification also may be obtained, for example, by having the individual sign a separate list or simply initial a cover sheet of the notice to be retained by the covered entity. The proposal would not limit the manner in which a covered entity obtains the individual's acknowledgment of receipt of the notice.

Most importantly, the proposed modification would require only the good faith effort of the provider to obtain the individual's acknowledgment. The Department understands that an individual may refuse to sign or otherwise fail to provide his or her acknowledgment. Unlike the Privacy Rule's consent requirement, an individual's failure or refusal to acknowledge the notice, despite a covered entity's good faith efforts to obtain such signature, would not interfere with the provider's ability to deliver timely and effective treatment. Failure by a covered entity to obtain an individual's acknowledgment,

assuming it otherwise documented its good faith effort, would not be considered a violation of the Privacy Rule. Compliance with this requirement would be achieved in a particular case if the provider with a direct treatment relationship either: (1) obtained a written acknowledgment, or (2) made a good faith effort to obtain such acknowledgment and documented such efforts and the reason for failure. Such reason for failure simply may be, for example, that the individual refused to sign after being requested to do so. In addition to the individual's failure or refusal to acknowledge receipt of the notice, this proposed provision is intended to allow covered health care providers flexibility to deal with a variety of circumstances in which obtaining an acknowledgment is problematic.

The requirement for a good faith effort to obtain the individual's acknowledgment would apply, except in emergency treatment situations, to the provision of notice on the first delivery of service, regardless of whether such service is provided in person or electronically. When electronic notice is provided as part of the first service delivery, the system should be capable of capturing the individual's acknowledgment of receipt electronically. The Department does not anticipate that a notification of receipt would be difficult or costly to design.

Documentation requirements under this proposal would be required to comply with the documentation requirements in § 164.530(j). In addition, nothing in the proposed requirements described above would relieve any covered entity from its duty to provide the notice in plain language so that the average reader can understand the notice. As stated in the preamble to the Privacy Rule, the Department encourages covered entities to consider alternative means of communicating with certain populations, such as with

individuals who cannot read or who have limited English proficiency.

C. Minimum Necessary and Oral Communications

The Privacy Rule at § 164.502(b) generally requires covered entities to make reasonable efforts to limit the use or disclosure of, and requests for, protected health information to the minimum necessary to accomplish the intended purpose. Protected health information includes individually identifiable health information in any form, including information transmitted orally, or in written or electronic form. See the definition of "protected health information" at § 164.501. The minimum necessary standard is intended to make covered entities evaluate their practices and enhance protections as needed to limit unnecessary or inappropriate access to, and disclosures of, protected health information.

The Privacy Rule sets forth requirements at § 164.514(d) for implementing the minimum necessary standard with regard to a covered entity's uses, disclosures, and requests. Essentially, a covered entity is required to develop and implement policies and procedures appropriate to the entity's business practices and workforce that reasonably minimize the amount of protected health information used, disclosed, and requested; and, for uses of protected health information, that also limit who has access to such information. Specifically, for uses of protected health information, the policies and procedures must identify the persons or classes of persons within the covered entity who need access to the information to carry out their job duties, the categories or types of protected health information needed, and conditions appropriate to such access. For

routine or recurring requests and disclosures, the policies and procedures may be standard protocols. Non-routine requests for and disclosures of protected health information must be reviewed individually.

With regard to disclosures, the Privacy Rule permits a covered entity to rely on the judgment of certain parties requesting the disclosure as to the minimum amount of information that is needed. For example, a covered entity is permitted to reasonably rely on representation from a public health official that the protected health information requested is the minimum necessary for a public health purpose. Similarly, a covered entity is permitted to reasonably rely on the judgment of another covered entity requesting a disclosure that the information requested is the minimum amount of information reasonably necessary to fulfill the purpose for which the request has been made. See § 164.514(d)(3)(iii).

The Privacy Rule contains some exceptions to the minimum necessary standard. The minimum necessary requirements do not apply to uses or disclosures that are required by law, disclosures made to the individual or pursuant to an authorization initiated by the individual, disclosures to or requests by a health care provider for treatment purposes, uses or disclosures that are required for compliance with the regulations implementing the other administrative simplification provisions of HIPAA, or disclosures to the Secretary of HHS for enforcement purposes. See § 164.502(b)(2).

The Department received much, varied commentary both on the minimum necessary provisions, as well as on the Privacy Rule's protections of oral communications. The following discussion addresses the concerns identified by commenters that were

common to both the Privacy Rule's standards for minimum necessary as well as protecting oral communications, and describes the Department's proposal for modifying the Privacy Rule in response to these concerns. In addition, the Department proposes to modify certain other paragraphs within § 164.514(d) to clarify the Department's intent with respect to these provisions. The Department also discusses some of the other concerns that have been received, which the Department attempted to address in its July 6 guidance on the Privacy Rule. Lastly, the Department describes the recommendations provided to the Department by the NCVHS as a result of public testimony received on implementation of the minimum necessary standard, as well as the Department's response to these recommendations.

Public Comments – Incidental Uses and Disclosures

During the March 2001, comment period on the Privacy Rule, the Department received a number of comments raising concerns and questions as to whether the Privacy Rule's restrictions on uses and disclosures will prohibit covered entities from engaging in certain common and essential health care communications and practices in use today. Commenters were concerned that the Department is imposing through the Privacy Rule absolute, strict standards that would not allow for the incidental or unintentional disclosure that could occur as a by-product of engaging in these health care communications and practices. It was argued that the Privacy Rule will, in effect, prohibit such practices and, therefore, impede many activities and communications essential to effective and timely treatment of patients.

These concerns were raised both in the context of applying the Privacy Rule's protections to oral communications, as well as in implementing the minimum necessary standard. For example, with regard to oral communications, commenters expressed concern over whether health care providers may continue to engage in confidential conversations with other providers or with patients, if there were a possibility that they could be overheard. As examples, commenters specifically questioned whether health care staff can continue to: coordinate services at hospital nursing stations orally; discuss a patient's condition over the phone with the patient or another provider, if other people are nearby; discuss lab test results with a patient or other provider in a joint treatment area; call out a patient's name in a waiting room; or discuss a patient's condition during training rounds in an academic or training institution.

Many covered entities also expressed confusion and concern that the Privacy Rule will stifle or unnecessarily burden many of their current health care practices. For example, commenters questioned whether they will be prohibited from using sign-in sheets in waiting rooms or maintaining patient charts at bedside, or whether they will need to isolate X-ray lightboards or destroy empty prescription vials. These concerns seemed to stem from a perception that covered entities will be required to prevent any incidental disclosure such as those that may occur when a visiting family member or other person not authorized to access protected health information happens to walk by medical equipment or other material containing individually identifiable health information, or when individuals in a waiting room sign their name on a log sheet and glimpse the names of other patients.

Proposed Modifications – Incidental Uses and Disclosures

The Department, in its July 6 guidance, clarified that the Privacy Rule is not intended to impede customary and necessary health care communications or practices, nor to require that all risk of incidental use or disclosure be eliminated to satisfy its standards. So long as reasonable safeguards are employed, the burden of impeding such communications are not outweighed by any benefits that may accrue to individuals' privacy interests. The guidance assured that the Privacy Rule would be modified to clarify that such communications and practices may continue, if reasonable safeguards are taken to minimize the chance of incidental disclosure to others.

Accordingly, the Department proposes to modify the Privacy Rule to add a new provision at § 164.502(a)(1)(iii) which explicitly permits certain incidental uses and disclosures that occur as a result of an otherwise permitted use or disclosure under the Privacy Rule. An incidental use or disclosure would be a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a by-product of an otherwise permitted use or disclosure under the Privacy Rule. The Department proposes that an incidental use or disclosure be permissible only to the extent that the covered entity has applied reasonable safeguards as required by § 164.530(c), and implemented the minimum necessary standard, where applicable, as required by §§ 164.502(b) and 164.514(d).

Under this proposal, an incidental use or disclosure that occurs as a result of a failure to apply reasonable safeguards or the minimum necessary standard, as appropriate, is not a permissible use or disclosure and is, therefore, a violation of the Privacy Rule. For

example, a covered entity that asks for a patient's health history on the waiting room sign-in sheet is not abiding by the minimum necessary requirements and, therefore, any incidental disclosure of such information that results from this practice would be an unlawful disclosure under the Privacy Rule.

Further, this proposed modification is not intended to excuse erroneous uses or disclosures or those that result from mistake or neglect. The Department would not consider such uses and disclosures to be incidental as they do not occur as a by-product of an otherwise permissible use or disclosure. For example, an impermissible disclosure would occur when a covered entity mistakenly sends protected health information via electronic mail to the wrong recipient or when protected health information is erroneously made accessible to others through the entity's web site.

Proposed Modifications to the Minimum Necessary Standard

Section 164.502(b)(2) sets forth the exceptions to the minimum necessary standard in the Privacy Rule. The Department proposes to separate § 164.502(b)(2)(ii) into two subparagraphs (§ 164.502(b)(2)(ii) and (iii)) to eliminate confusion regarding the exception to the minimum necessary standard for uses or disclosures made pursuant to an authorization under § 164.508 and those for disclosures made to the individual. Additionally, to conform to the proposal to eliminate the special authorizations required by the Privacy Rule at § 164.508(d), (e), and (f) (see section III.H for the relevant preamble discussion regarding authorization), the Department proposes to expand the exception for authorizations to apply generally to any authorization executed pursuant to

§ 164.508. Therefore, the proposal would exempt from the minimum necessary standard any uses or disclosures for which the covered entity has received an authorization that meets the requirements of § 164.508.

The Privacy Rule at § 164.514(d) lists the standard and the specific requirements for implementing the minimum necessary standard. The Department proposes to modify § 164.514(d)(1) to delete the term "reasonably ensure" in response to concerns that the term connotes an absolute, strict standard and, therefore, is inconsistent with how the Department has described the minimum necessary requirements as being reasonable and flexible to the unique circumstances of the covered entity. In addition, the Department generally revises the language to be more consistent with the description of standards elsewhere in the Privacy Rule.

The Privacy Rule at § 164.514(d)(4) consists of the implementation specifications for applying the minimum necessary standard to a request for protected health information. The Department intended these provisions to be consistent with the requirements set forth in § 164.514(d)(3) for applying the minimum necessary standard to disclosures of protected health information, so that covered entities would be able to address requests and disclosures in a similar manner. However, with respect to requests not made on a routine and recurring basis, the Department omitted from § 164.514(d)(4) the requirement that a covered entity may implement this standard by developing criteria designed to limit its request for protected health information to the minimum necessary to accomplish the intended purpose. The Department proposes to add such a provision to make the implementation specifications for applying the minimum necessary standard to

requests for protected health information by a covered entity more consistent with the implementation specifications for disclosures.

Other Comments on the Minimum Necessary Standard

In addition to the comments described above regarding incidental uses or disclosures, the Department received many other varied comments expressing both support of, and concerns about, the minimum necessary standard. The Department, in its July 6, 2001, guidance, attempted to address many of the commenters' concerns by clarifying the Department's intent with respect to the minimum necessary provisions. For example, many commenters expressed concerns about the costs and burden to covered entities in implementing the standard. A number of these commenters questioned whether they will be required to redesign office space or implement expensive upgrades to computer systems.

The Department's guidance emphasized that the minimum necessary standard is a reasonableness standard, intended to be flexible to account for the characteristics of the entity's business and workforce. The standard is not intended to override the professional judgment of the covered entity. The Department clarified that facility redesigns and expensive computer upgrades are not specifically required by the minimum necessary standard. Covered entities may, however, need to make certain adjustments to their facilities, as reasonable, to minimize access or provide additional security. For example, covered entities may decide to isolate and/or lock file cabinets or records rooms, or provide additional security, such as passwords, on computers that maintain protected

health information.

A number of commenters, especially health care providers, also expressed concern that the minimum necessary restrictions on uses within the entity will jeopardize patient care and exacerbate medical errors by impeding access to information necessary for treatment purposes. These commenters urged the Department to expand the treatment exception to cover uses of protected health information within the entity. Other commenters urged the Department to exempt all uses and disclosures for treatment, payment, and health care operations purposes from the minimum necessary standard.

The Privacy Rule is not intended to impede access by health care professionals to information necessary for treatment purposes. As the Department explained in its guidance, a covered entity is permitted to develop policies and procedures that allow for the appropriate individuals within the entity to have access to protected health information, including entire medical records, as appropriate, so that those workforce members are able to provide timely and effective treatment.

With regard to payment and health care operations, the Department remains concerned, as stated in the preamble to the Privacy Rule, that, without the minimum necessary standard, covered entities may be tempted to disclose an entire medical record when only a few items of information are necessary, to avoid the administrative step of extracting or redacting information. The Department also believes that this standard will cause covered entities to assess their privacy practices, give the privacy interests of their patients and enrollees greater attention, and make improvements that might otherwise not be made. For these reasons, the Department continues to believe that the privacy benefits

of retaining the minimum necessary standard for these purposes outweigh the burdens involved.

In addition, the NCVHS Subcommittee on Privacy and Confidentiality solicited public testimony on implementation of the minimum necessary standard of the Privacy Rule at its August 2001 public hearings. The testimony reflected a wide range of views, from those who commented that the Privacy Rule provides sufficient protections on individually identifiable health information without the minimum necessary standard, to those who expressed strong support for the standard as an integral part of the Privacy Rule. A number of panelists welcomed the flexibility of the standard, while others expressed concern that the vagueness of the standard might restrict the necessary flow of information, impede care, and lead to an increase in defensive information practices that would lead to the withholding of important information for fear of liability. Testimony also reflected differing views on the cost and administrative burden of implementing the standard. Some expressed much concern regarding the increased cost and burden, while others argued that the cost will be barely discernable.

The NCVHS developed recommendations on the minimum necessary standard based on the testimony and written comments provided at the hearings. In its recommendations, the NCVHS strongly reaffirmed the importance of the minimum necessary principle, but also generally recommended that HHS provide additional clarification and guidance to industry regarding the minimum necessary requirements to assist with effective implementation of these provisions, while allowing for the necessary flow of information and minimizing defensive information practices. While the NCVHS

pointed out that many panelists at the hearing found the Department's July 6 guidance helpful in addressing questions about the minimum necessary standard, the Committee heard that many questions still remain within the industry. Therefore, the NCVHS specifically requested further guidance by the Department on the reasonable reliance provisions, and the requirement that covered entities develop policies and procedures for addressing routine uses of information. In addition, the NCVHS recommended that the Department provide education to address the increasing concerns about liability and defensive information practices that may lessen the flow of information and impede care. The NCVHS generally recommended that the Department issue advisory opinions, publish best practices, and make available model policies, procedures, and forms to assist in alleviating the cost and administrative burden that will be incurred when developing policies and procedures as required by the minimum necessary provisions.

The Department agrees with the NCVHS about the need for further guidance on the minimum necessary standard and intends to issue further guidance to clarify issues causing confusion and concern in the industry, as well as provide additional technical assistance materials to help covered entities implement the provisions.

D. Business Associates

The Privacy Rule at § 164.502(e) permits a covered entity to disclose protected health information to a business associate who performs a function or activity on behalf of, or provides a service to the covered entity that involves the creation, use, or disclosure of, protected health information, provided that the covered entity obtains satisfactory

assurances that the business associate will appropriately safeguard the information. The Department recognizes that most covered entities do not perform or carry out all of their health care activities and functions by themselves, but rather acquire the services or assistance of a variety of other persons or entities. Given this framework, the Department intended these provisions to allow such business relationships to continue while ensuring that identifiable health information created or shared in the course of the relationships was protected.

The Privacy Rule requires that the satisfactory assurances obtained from the business associate be in the form of a written contract (or other written arrangement as between governmental entities) between the covered entity and the business associate that contains the elements specified at § 164.504(e). For example, the agreement must identify the uses and disclosures of protected health information the business associate is permitted or required to make, as well as require the business associate to put in place appropriate safeguards to protect against a use or disclosure not permitted by the contract or agreement.

The Privacy Rule also provides that, where a covered entity knows of a material breach or violation by the business associate of the contract or agreement, the covered entity is required to take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, to terminate the contract or arrangement. If termination of the contract or arrangement is not feasible, a covered entity then is required to report the problem to the Secretary of HHS. A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in

noncompliance with the Privacy Rule's business associate provisions.

The Privacy Rule's definition of "business associate" at § 160.103 includes some of the functions or activities, and all of the types of services, that make a person or entity who engages in them a business associate, if such activity or service involves protected health information. For example, a third party administrator (TPA) is a business associate of a health plan to the extent the TPA assists the health plan with claims processing or another covered function. Similarly, accounting services performed by an outside consultant give rise to a business associate relationship when provision of the service entails access to the protected health information held by a covered entity.

The Privacy Rule excepts from the business associate standard certain uses or disclosures of protected health information. That is, in certain situations, a covered entity is not required to have a contract or other written agreement in place before disclosing protected health information to a business associate or allowing protected health information to be created by the business associate on its behalf. Specifically, the standard does not apply to: disclosures by a covered entity to a health care provider for treatment purposes; disclosures to the plan sponsor by a group health plan, or a health insurance issuer or HMO with respect to a group health plan, to the extent that the requirements of § 164.504(f) apply and are met; or to the collection and sharing of protected health information by a health plan that is a public benefits program and an agency other than the agency administering the health plan, where the other agency collects protected health information for, or determines, eligibility or enrollment with respect to the government program, and where such activity is authorized by law. See § 164.502(e)(1)(ii).

Public Comments

The Department has received many comments on the business associate provisions of the Privacy Rule. The majority of commenters expressed some concern over the anticipated administrative burden and cost to implement the business associate provisions. Some commenters stated that covered entities might have existing contracts that are not set to terminate or expire until after the compliance date of the Privacy Rule. Many of these commenters expressed specific concern that the two-year compliance period does not provide enough time to reopen and renegotiate what could be hundreds or more contracts for large covered entities. A number of these commenters urged the Department to grandfather in existing contracts until such contracts come up for renewal instead of requiring that all contracts be in compliance with the business associate provisions by the compliance date of the Privacy Rule. In response to these comments, the Department intends to relieve some of the burden on covered entities in complying with the business associate provisions, both by proposing to grandfather certain existing contracts for a specified period of time, as well as publishing model contract language. These proposed changes are discussed below in this section under "Proposed Modifications."

In addition, commenters continued to express concern over a perceived liability imposed by the Privacy Rule that would essentially require that the covered entity monitor, and be responsible for, the actions of its business associates with respect to the privacy and safeguarding of protected health information. However, the Privacy Rule only requires that, where a covered entity knows of a pattern of activity or practice that constitutes a material breach or violation of the business associate's obligation under the