Federal Register

Wednesday,
March 27, 2002

Part II

Department of Health and Human Services

45 CFR Parts 160 and 164
Office of the Secretary; Standards for Privacy of Individually Identifiable Health Information; Proposed Rule

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 April 26, 2002, 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 April 26, 2002.

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 Web site: *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 3½ 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 to 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 contract, the covered entity take steps to cure the breach or end the violation. Accordingly, the Department, in its July 6 guidance, clarified that active monitoring of the actions of business associates is not required of covered entities, and more importantly, that covered entities are not responsible or liable for the actions of their business associates.

A number of commenters urged the Department to exempt covered entities from having to enter into contracts with business associates who are also covered entities under the Privacy Rule. The Department continues to believe, as stated in the preamble to the Privacy Rule, that a covered entity that is a

business associate should be restricted from using or disclosing the protected health information it creates or receives through its business associate function for any purposes other than those explicitly provided for in its contract. In addition, the contract serves to clarify the uses and disclosures made as, and the protected health information held by, the covered entity, versus those uses and disclosures made as, and the protected health information held by, the same entity as the business associate.

Many commenters continued to express concerns that requiring business associate contracts between health care providers in treatment situations would burden and impede quality care. The Department clarifies that the Privacy Rule does not require a contract for a covered entity to disclose protected health information to a health care provider for treatment purposes. In fact, such disclosures are explicitly excepted from the business associate requirements. *See* § 164.502(e)(1). For example, a hospital is not required to have business associate contracts with health care providers who have staff privileges at the institution in order for these entities to share protected health information for treatment purposes. Nor is a physician required to have a business associate contract with a laboratory as a condition of disclosing protected health information for the treatment of an individual.

Some commenters requested clarification as to whether business associate contracts were required between a health plan and the health care providers participating in the plan's network. Participation in a plan network in and of itself does not give rise to a business associate relationship to the extent that neither entity is performing functions or activities, or providing services to, the other entity. For example, each covered entity is acting on its own behalf when a provider submits a claim to a health plan, and when the health plan assesses and pays the claim. Discount payment arrangements do not require business associate relationships. However, this does not preclude a covered entity from establishing a business associate relationship with the health plan or another entity in the network for some other purpose. If the health plan and one or more of the providers participating in its network do perform covered functions on behalf of each other, a business associate agreement is required. For example, if one health care provider handles the billing activities of another health care provider in the same network, a business associate contract would be required before protected health information could be disclosed for this activity.

Proposed Modifications

The Department proposes new transition provisions at § 164.532(d) and (e) to allow covered entities, other than small health plans, to continue to operate under certain existing contracts with business associates for up to one year beyond the April 14, 2003, compliance date of the Privacy Rule. This modification is proposed in response to commenter concerns regarding the insufficient time provided by the two-year period between the effective date and compliance date of the Privacy Rule for covered entities, especially large entities, to reopen and renegotiate all existing vendor and service contracts in order to bring such contracts into compliance with the Privacy Rule's requirements.

The additional transition period would be available to a covered entity, other than a small health plan, if, prior to the effective date of this transition provision, the covered entity has an existing contract or other written arrangement with a business associate, and such contract or arrangement is not renewed or modified between the effective date of this provision and the Privacy Rule's compliance date of April 14, 2003. The provisions are intended to allow those covered entities who qualify as described above to continue to disclose protected health information to the business associate, or allow the business associate to create or receive protected health information on its behalf, for up to one year beyond the Privacy Rule's compliance date, regardless of whether the contract meets the applicable contract requirements in the Privacy Rule. The Department proposes to deem such contracts to be compliant with the Privacy Rule until either the covered entity has renewed or modified the contract following the compliance date of the Privacy Rule (April 14, 2003), or April 14, 2004, whichever is sooner. In cases where a contract simply renews automatically without any change in terms or other action by the parties (also known as ''evergreen contracts''), the Department intends that such evergreen contracts would be eligible for the extension and that deemed compliance would not terminate when these contracts automatically roll over.

Covered entities that were concerned about timely compliance wanted to be able to incorporate the business associate contract requirements at the time they would otherwise be modifying or renewing the contract. Therefore, the extension would only apply until such time as the contract is modified or renewed following the effective date of this modification. Furthermore, the Department proposes to limit the deemed compliance period to one year, as the appropriate balance between maintaining individuals' privacy interests and alleviating the burden on the covered entity.

These transition provisions would apply to covered entities only with respect to written contracts or other written arrangements as specified above, and not to oral contracts or other arrangements. In addition, a covered entity that enters into a contract after the effective date of this modification must have a business associate contract that meets the applicable requirements of §§ 164.502(e) and 164.504(e) by April 14, 2003.

The proposed transition provisions would not apply to small health plans, as defined in the Privacy Rule. Small health plans would still be required to have business associate contracts that are in compliance with the Privacy Rule's applicable provisions, by the Privacy Rule's compliance deadline for such covered entities of April 14, 2004. The Department proposes to exclude this subset of covered entities from these provisions because the statute already provides an additional year for these smaller entities to come into compliance, which should be sufficient for compliance with the Privacy Rule's business associate provisions. In addition, the Department believes that the proposed model contract provisions (see the Appendix to the preamble) will assist small health plans and other covered entities in their implementation of the Privacy Rule's business associate provisions by April 14, 2004.

Proposed § 164.532(e)(2) provides that, after the Privacy Rule's compliance date, these new provisions would not relieve a covered entity of its responsibilities with respect to making protected health information available to the Secretary, including information held by a business associate, as necessary for the Secretary to determine compliance. Similarly, under proposed § 164.532(e)(2), these provisions would not relieve a covered entity of its responsibilities with respect to an individual's rights to access or amend his or her protected health information held by business associates, or receive an accounting of uses and disclosures by business associates, as provided for by the Privacy Rule's requirements at §§ 164.524, 164.526, and 164.528. Covered entities would still be required to fulfill individuals' rights with respect to their protected health information,

including information held by a business associate of the covered entity. Covered entities must ensure, in whatever manner effective, the appropriate cooperation by their business associates in meeting these requirements.

The Department retains without modification the standards and implementation specifications that apply to business associate relationships as set forth at §§ 164.502(e) and 164.504(e), respectively, of the Privacy Rule.

E. Uses and Disclosures of Protected Health Information for Marketing

The Privacy Rule defines ''marketing'' at § 164.501 as a communication about a product or service, a purpose of which is to encourage recipients of the communication to purchase or use the product or service, subject to certain limited exceptions. The definition does not limit the type or means of communication that is considered marketing. In general, a covered entity is not permitted to use or disclose protected health information for the purposes of marketing products or services that are not health-related without the express authorization of the individual. Moreover, the Privacy Rule prohibits a covered entity from selling lists of patients or enrollees to third parties, or from disclosing protected health information to a third party for the independent marketing activities of the third party, without the express authorization of the individual.

The Department understands that covered entities need to be able to discuss their own health-related products and services, or those of third parties, as part of their everyday business and as part of promoting the health of their patients and enrollees. For example, a health care provider may recommend to a patient a particular brand name drug for the treatment of that patient. Even though these communications also meet the above definition of ''marketing,'' the Privacy Rule does not require an authorization for such communications. Instead, the Privacy Rule addresses these types of health-related communications in two ways.

First, the Department did not want to interfere with or unnecessarily burden communications about treatment or about the benefits and services of plans and providers. Therefore, the Privacy Rule explicitly excludes from the definition of ''marketing'' certain health-related communications that may be part of a covered entity's treatment of the individual or its health care operations, but that may also promote the use or sale of a service or product. For example, communications made by a covered entity for the purpose of describing the participating providers and health plans in a network, or describing the services offered by a provider or the benefits covered by a health plan, are excluded from the definition of ''marketing.'' In addition, communications made by a health care provider as part of the treatment of a patient and for the purpose of furthering that treatment, or made by a covered entity in the course of managing an individual's treatment or recommending an alternative treatment, are not considered marketing under the Privacy Rule. These exceptions do not apply, however, to written communications for which a covered entity is compensated by a third party. The Department intended that covered entities be able to discuss freely their products and services and the products and services of others in the course of managing an individual's health care or providing or discussing treatment alternatives with an individual. Under the Privacy Rule, therefore, covered entities are permitted to use and disclose protected health information for these excepted activities without authorization under § 164.508.

Second, the Privacy Rule permits, at § 164.514(e), covered entities to use and disclose protected health information without individual authorization for other health-related communications that meet the definition of ''marketing,'' subject to certain conditions on the manner in which the communications are made. The Privacy Rule does not condition the substance of health-related marketing communications. Rather, it attempts to assure that individuals are aware of the source of the communication and the reason they received such communications, as well as to provide individuals with some control over whether or not they receive these communications in the future.

Specifically, the Privacy Rule permits a covered entity to use or disclose protected health information to communicate to individuals about the health-related products or services of the covered entity or of a third party if the communication: (1) Identifies the covered entity as the party making the communication; (2) identifies, if applicable, that the covered entity received direct or indirect remuneration from a third party for making the communication; (3) generally contains instructions describing how the individual may opt out of receiving future communications about health-related products and services; and (4) where protected health information is used to target the communication about a product or service to individuals based on their health status or health condition, explains why the individual has been targeted and how the product or service relates to the health of the individual. The Privacy Rule also requires a covered entity to make a determination, prior to using or disclosing protected health information to target a communication to individuals based on their health status or condition, that the product or service may be beneficial to the health of the type or class of individual targeted to receive the communication.

For certain permissible marketing communications, however, the Department did not believe these conditions to be practicable. Therefore, § 164.514(e) also permits, without the above conditions, a covered entity to make a marketing communication that occurs in a face-to-face encounter with the individual, or that involves products or services of only nominal value. These provisions permit a covered entity to discuss services and products, as well as provide sample products without restriction, during a face-to-face communication, or distribute calendars, pens, and other merchandise that generally promote a product or service if they are of only nominal value.

Public Comments

The Department received many comments on the Privacy Rule's marketing requirements, as well as recommendations from the NCVHS, based on public testimony from trade associations, medical associations, insurance commissioners, academic medical centers, non-profit hospitals, and consumers. Both industry and consumer groups argued that the marketing provisions were complicated and confusing. Covered entities expressed confusion over the Privacy Rule's distinction between health care communications that are excepted from the definition of ''marketing'' versus those that are marketing but permitted subject to the special conditions in § 164.514(e). For example, commenters questioned if, and if so, when, disease management communications or refill reminders are ''marketing'' communications subject to the special disclosure and opt-out conditions in § 164.514(e). Commenters also stated that it was unclear how to characterize various health care operations activities, such as general health-related educational and wellness promotional activities, and therefore unclear how to treat such activities under the marketing provisions of the Privacy Rule.

The Department also learned of a general dissatisfaction by consumers

with the conditions required by § 164.514(e). Many commenters questioned the general effectiveness of the conditions and whether the conditions would properly protect consumers from unwanted disclosure of protected health information to commercial entities, the re-disclosure of the information by these commercial entities, and the intrusion of unwanted solicitations. They did not feel that they were protected by the fact that commercial entities handling the protected health information would be subject to business associate agreements with covered entities. In addition, commenters expressed specific dissatisfaction with the provision at § 164.514(e)(3)(iii) for individuals to opt out of future marketing communications. Many argued for the opportunity to opt out of marketing communications before any marketing occurred. Others requested that the Department limit marketing communications to only those consumers that affirmatively chose to be the target of such communications.

Proposed Modifications

In response to these concerns, the Department proposes to modify the Privacy Rule to make the marketing provisions clearer and simpler. First, and most significantly, the Department proposes to simplify the Privacy Rule by eliminating the special provisions for marketing health-related products and services at § 164.514(e). Instead, any communication defined as ''marketing'' in § 164.501 would require authorization by the individual. In contrast to the Privacy Rule, under these proposed modifications, covered entities would no longer be able to make any type of marketing communications without authorization simply by meeting the disclosure and opt-out provisions in the Privacy Rule. The Department believes that requiring authorization for all marketing communications would effectuate greater consumer privacy protection not currently afforded by the disclosure and opt-out conditions of § 164.514(e) of the Privacy Rule.

Second, the Department proposes to maintain the substance of the Privacy Rule's definition of ''marketing'' at § 164.501, with minor clarifications. Specifically, the Department proposes to define ''marketing'' as ''to make a communication about a product or service to encourage recipients of the communication to purchase or use the product or service.'' The proposed modification retains the substance of the ''marketing'' definition, but changes the language slightly to avoid the implication that marketing is tied to the intent of the communication. Removing language referencing the purpose of the communication would shift the assessment of whether a communication is marketing from the intent of the speaker to the effect of the communication. If the effect of the communication is to encourage recipients of the communication to purchase or use the product or service, the communication would be marketing.

Third, with respect to the exclusions from the definition of ''marketing'' in § 164.501, the Department has tried to simplify the language to avoid confusion and better conform to other sections of the regulation, particularly in the area of treatment communications, and is proposing one substantive change. The modified language reads as follows: ''(1) To describe the entities participating in a health care provider network or health plan network, or to describe if, and the extent to which, a product or service (or payment for such product or service) is provided by a covered entity or included in a plan of benefits; (2) For treatment of that individual; or (3) For case management or care coordination for that individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to that individual.''

With respect to the third exclusion, the Department is proposing to replace a communication made ''in the course of managing the treatment of that individual,'' with a communication for ''case management'' or ''care coordination'' for that individual. The Department is proposing these changes for clarity because ''case management'' and ''care coordination'' are the terms that are used in the definition of ''health care operations,'' while ''managing the treatment of that individual'' is not. These changes are not intended to increase the scope of the marketing exclusions.

The Department is proposing to eliminate the distinction in the definition of ''marketing'' at § 164.501 pertaining to written communications for which a covered entity is compensated by a third party. Under the Privacy Rule, exceptions from the definition of ''marketing'' are only applicable if the communication is made either orally or in writing when no remuneration from a third party has been paid to a covered entity for making the communication. The Department found that these rules led to confusion and many questions about treatment-related communications, such as prescription refill reminders. Many commenters felt that these restriction rules could burden the ability of providers and patients to communicate freely about treatment. Most commenters did not want any treatment communications to be considered marketing. The Department understands these concerns and wants to avoid situations where a health care provider would be required to obtain an authorization to send out a prescription refill reminder, even if the provider is compensated by a third party for the activity. Therefore, the Department proposes to eliminate this provision in order to facilitate necessary and important treatment communications.

None of these proposed modifications change the basic prohibition in the Privacy Rule against covered entities selling lists of patients or enrollees to third parties, or from disclosing protected health information to a third party for the independent marketing activities of a third party, without the express authorization of the individual.

The Department received numerous comments suggesting that the Privacy Rule's marketing exceptions in the definition and under § 164.514(e) may not allow for certain common health care communications, such as disease management, wellness programs, prescription refill reminders, and appointment notifications that individuals expect to receive as part of their health care to continue unimpeded. The Department believes that these types of communications are allowed under the exceptions to the definition of ''marketing'' in the Privacy Rule, and therefore would continue to be allowed under the proposed modification. The Department is interested in comments identifying specific types of communication that should or should not be considered marketing.

To reinforce the policy requiring an authorization for most marketing communications, the Department proposes to add a specific marketing provision at § 164.508(a)(3) explicitly requiring an authorization for a use or disclosure of protected health information for marketing purposes. Additionally, if the marketing is expected to result in direct or indirect remuneration to the covered entity from a third party, the Department proposes that the authorization state this fact. As in the Privacy Rule at § 164.514(e)(2), proposed § 164.508(a)(3) would exclude from the marketing authorization requirements face-to-face communications made by a covered entity to an individual. The Department proposes to retain this exception in the Privacy Rule so that the marketing provisions would not interfere with the

relationship and dialogue between health care providers and individuals. Similarly, the Department proposes to retain the Privacy Rule's exception to the authorization requirement for a marketing communication that concerns products or services of nominal value, but proposes to replace the language with the common business term ''promotional gift of nominal value.''

Given the above proposal, the Department also proposes to remove § 164.514(e) as unnecessary. Accordingly, conforming changes to remove references to § 164.514(e) are proposed at § 164.502(a)(1)(vi) and in paragraph (6)(v) of the definition of ''health care operations'' in § 164.501.

With the elimination of the special rules in § 164.514(e), the Department thereby proposes to eliminate the requirement that disclosures for health-related marketing are limited to disclosures to business associates hired to assist the covered entity with the communication. Under the proposed rule, this distinction would serve no purpose, because an authorization would be required for such disclosures and thus the individual would know from the face of the authorization who will receive the information. Similarly, this simplification also would eliminate the requirement that a marketing communication identify the covered entity responsible for the communication. Under the proposal, the individual would have authorized the disclosure and thus would know which plans and providers are disclosing health information for marketing purposes. There would be added burden but no benefit in retaining an additional notification requirement.

F. Parents as Personal Representatives of Unemancipated Minors [1]

The Privacy Rule is intended to assure that parents have appropriate access to health information about their children. By generally creating new protections and individual rights with respect to individually identifiable health information, the Privacy Rule establishes new rights for parents with respect to the health information about their minor children in the vast majority of cases. In addition, the Department intended that State or other applicable law regarding disclosure of health information about a minor child to a parent should govern where such law exists.

Under the Privacy Rule, parents are granted new rights with respect to health information about their minor children as the personal representatives of their minor children. See § 164.502(g). Generally, parents will be able to access and control the health information about their minor children. See § 164.502(g)(3).

The Privacy Rule recognizes a limited number of exceptions to this general rule. These exceptions generally track the ability of certain minors to obtain specified health care without parental consent under State or other applicable laws. For example, every State has a law that permits adolescents to be tested for HIV without the consent of a parent. These laws are created to assure that adolescents will seek health care that is essential to their own health, as well as public health. In these exceptional cases, where a minor can obtain a particular health care service without the consent of a parent under State or other applicable law, it is the minor and not the parent who may exercise the privacy rights afforded to individuals under the Privacy Rule. See § 164.502(g)(3)(i)–(ii).

The Privacy Rule also allows the minor to exercise control of the protected health information when the parent has agreed to the minor obtaining confidential treatment (see § 164.502(g)(3)(iii)), and allows a covered health care provider to choose not to treat a parent as a personal representative of the minor when the provider is concerned about abuse or harm to the child. See § 164.502(g)(5).

Of course, a covered provider always may disclose health information about a minor to a parent in the most important cases, even if one of the limited exceptions discussed above apply. Disclosure of such information is always permitted as necessary to avert a serious and imminent threat to the health or safety of the minor. See § 164.512(j). The Privacy Rule also states that disclosure of health information about a minor to a parent is permitted if State law authorizes or requires disclosure to a parent, thereby allowing such disclosure where State law determines it is appropriate. See § 160.202, definition of ''more stringent.'' Finally, health information about the minor may be disclosed to the parent if the minor involves the parent in his or her health care and does not object to such disclosure. See §§ 164.502(g)(3)(i) and 164.510(b). The parent will retain all rights concerning any other health information about his or her minor child that does not meet one of the exceptions.

Rationale for Privacy Rule's Provisions Regarding Parents and Minors

The Department continues to balance multiple goals in developing standards in the Privacy Rule with respect to parents and minors. First, the standards need to operate in a way that facilitates access to quality health care. This is an overarching goal throughout the Privacy Rule and is equally important here. Thus, the Department wants to ensure that parents have appropriate access to the health information about their minor children to make important health care decisions about them. The Department also wants to make sure that the Privacy Rule does not interfere with a minor's ability to consent to and obtain health care under current State or other applicable law. Second, the Department does not want to interfere with State or other applicable laws related to competency or parental rights, in general, or the role of parents in making health care decisions about their minor children, in particular. Third, the Department does not want to interfere with the professional requirements of State medical boards or other ethical codes of health care providers with respect to confidentiality of health information or health care practices of such providers with respect to adolescent health care.

As a result of these competing goals, the Department's approach continues to be that the standards, implementation specifications, and requirements with respect to parents and minors defer to, and are consistent with, State or other applicable law and professional practice. Where State and other applicable law is silent, the Department has attempted to create standards that are consistent with such laws and that permit States the discretion to continue to decide the rights of parents and minors with respect to health information without interference from the federal Privacy Rule.

Public Comments

Since December 2000, the Department has heard concerns about the impact of the Privacy Rule on both parental and minor rights. Physicians and other health care professionals who treat adolescents support the existing provisions in the Privacy Rule. These commenters assert that these provisions allow health care providers to deliver care in a manner consistent with their ethical and legal obligations, and that they strike the appropriate balance by permitting providers to render confidential care to minors in limited circumstances, while providing States

[1] Throughout this section of the preamble, ''minor'' refers to an unemancipated minor and ''parent'' refers to a parent, guardian, or other person acting *in loco parentis*.

the ultimate discretion to determine the extent of parents' access to information.

Other commenters oppose the Privacy Rule on the grounds that the Privacy Rule unduly interferes with parental rights to control health care for their minor children and to access health information about their minor children. They assert that failure to provide parents with access to all health information about their minor children could result in negative health outcomes because parents could be making health care decisions for their children based on incomplete information.

Finally, some commenters believe, incorrectly, that the Privacy Rule creates new rights for minors to consent to treatment. The Department issued guidance to clarify that the Privacy Rule does not address access to treatment or the ability to consent to treatment. It is State or other applicable law, and not the Privacy Rule, that governs who can consent to treatment. The Privacy Rule does not in any way alter the ability of a parent to consent to health care for a minor child or the ability of a minor child to consent to his or her own health care.

Proposed Modifications

The Department has reassessed the parents and minors provisions in the Privacy Rule, and does not propose to change its approach. The Department will continue to defer to State or other applicable law and to remain neutral and preserve the status quo to the extent possible. However, the Department is proposing changes to these standards where they do not operate as intended and are inconsistent with the Department's underlying goals.

The Privacy Rule accomplishes the goals of deferring to State law and preserving the status quo when State law is definitive, that is, when State law requires or prohibits disclosure or access. However, when State law provides discretion or is silent, the Privacy Rule may not always accomplish these goals. In particular, the Department has identified two areas in which the standard does not work as intended. First, the language regarding deference to State law that authorizes or prohibits disclosure of health information about a minor to a parent fails to assure that State law governs when the law grants a provider discretion to disclose protected health information to a parent in certain circumstances. Second, the Privacy Rule may prohibit parental access in cases where State law is silent, but where a parent could get access today, consistent with State law.

First, in order to assure that State and other applicable laws that address disclosure of health information about a minor to his or her parent govern in all cases, the Department proposes to move the relevant language about the disclosure of health information from the definition of ''more stringent'' (see § 160.202) to the standards regarding parents and minors (*see* § 164.502(g)(3)). This change would make it clear that State and other applicable law governs not only when a State explicitly addresses disclosure of protected health information to a parent but also when such law provides discretion to a provider.

The language itself is also changed in the proposal to adapt it to the new section. The proposed language in § 164.502(g)(3)(ii) states that a covered entity may disclose protected health information about a minor to a parent if an applicable provision of State or other law, including applicable case law, permits or requires such disclosure, and that a covered entity may not disclose protected health information about a minor to a parent if an applicable provision of State or other law, including applicable case law, prohibits such disclosure. This new language would help clarify when disclosure of health information about a minor to his or her parent is permitted or prohibited based on State or other law. The revision would also clarify that the deference to State or other applicable law includes deference to established case law as well as an explicit provision in a statute or regulation.

Second, the Department proposes to add a new paragraph (iii) to § 164.502(g)(3) to establish a neutral policy regarding the right of access of a parent to health information about a minor under § 164.524, in the rare circumstance in which the parent is technically not the personal representative of the minor under the Privacy Rule. This policy would apply particularly where State or other law is silent or unclear. The new paragraph would not change the right of access, but would simply provide that the person who can exercise the right of access to health information under the Privacy Rule must be consistent with State or other applicable law. It would assure that the Privacy Rule would not prevent a covered entity from providing such access, in accordance with the Privacy Rule, to a parent, as if a personal representative of the minor child, if access would be consistent with State or other applicable law.

This modification also would not affect a parent's right of access under the Privacy Rule in the vast majority of cases where the parent is the personal representative of the minor. In those cases, the parent could exercise the right of access in accordance with the Privacy Rule. This provision would be relevant only in the rare exceptions in which the parent is not the personal representative of the minor.

The Department proposes to use the phrase ''consistent with State or other applicable law'' with regard to access in the personal representatives section of the Privacy Rule. This is different than the proposed language in the section about personal representatives that relates to disclosures, in which a disclosure to a parent is permitted if such disclosure is permitted or required by an ''applicable provision of State or other law, including applicable case law.'' The language in the disclosure paragraphs requires an explicit law for such disclosure to be permitted by the Privacy Rule. The language in the access paragraphs permits parental access in accordance with the Privacy Rule if such access is consistent with State or other law, regardless of whether such law is explicit. Therefore, if a State permits a minor to obtain care without the consent of a parent, but is silent as to whether the parent can access the related medical records of the minor, as is typically the case, then the provider may provide access to the parent if such access is consistent with State law and could deny access to the parent if such denial of access is consistent with State law. This may be based on interpretation of State consent law or may be based on other law. The provider could not, however, abuse this provision to deny access to both the parent and the minor.

This provision would not significantly change the operation of the Privacy Rule with respect to parental access. In cases where the parent is not the personal representative of the minor under the Privacy Rule, the proposed language would not require a provider to grant access to a parent. In these cases, a provider would have discretion to provide access to a parent when permitted to do so under State or other applicable law despite the ability of the minor to obtain health care confidentially or without parental consent under applicable law or professional practice. The Department further assumes that current professional health care provider practices with respect to access by parents and confidentiality of minor's records are consistent with State and other applicable law. In any event, parental access under this section would continue to be subject to any relevant limitations on access in

§ 164.524. This proposed change provides States with the option of clarifying the interaction between their consent laws and the ability for parents to have access to the health information about the care that their minor children received in accordance with such laws. As such, this change should more accurately reflect current State law.

G. Uses and Disclosures for Research Purposes

1. Institutional Review Board (IRB) or Privacy Board Approval of a Waiver of Authorization

Much of the biomedical and behavioral research conducted in the U.S. is governed either by the rule entitled ''Federal Policy for the Protection of Human Subjects'' (the ''Common Rule'') and/or the Food and Drug Administration's (FDA) human subject protection regulations. Although these regulatory requirements, which apply to federally-funded and to some privately-funded research, include protections to help ensure the privacy of subjects and the confidentiality of information, the intent of the Privacy Rule, among other things, is to supplement these protections by requiring covered entities to implement specific measures to safeguard the privacy of individually identifiable health information.

The Common Rule applies to all human research that is supported, conducted, or regulated by any of the seventeen federal agencies that have adopted the Common Rule, including research that uses individually identifiable health information. FDA's human subject protection regulations generally apply to clinical investigations under FDA's jurisdiction, whether or not such research is federally funded. Both sets of regulations have requirements relating to review by an institutional review board (IRB) to ensure that the risks to research participants, including privacy risks, are minimized. As part of this review, generally, IRBs must consider the informed consent document that will be used to inform prospective research participants about the study. Both the Common Rule and FDA regulations have provisions relating to the waiver of informed consent. The Common Rule waiver provisions allow research covered by the Common Rule to be conducted if an IRB determines that certain criteria specified in the Common Rule have been met. FDA's regulations do not contain equivalent waiver provisions since the criteria for a waiver of informed consent are generally not appropriate for clinical research. However, FDA's human subject protection regulations contain exceptions to informed consent for emergency research and for the emergency use of an investigational product.

The Common Rule and FDA's regulations explicitly address privacy and confidentiality in the following places: (1) The informed consent document is required to include ''a statement describing the extent, if any, to which confidentiality of records identifying the subject will be maintained'' (Common Rule § ____.116(a)(5), 21 CFR 50.25(a)(5)); and (2) to approve a study an IRB must determine that ''when appropriate, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data'' (Common Rule § ____.111(a)(7), 21 CFR 56.111(a)(7)).

Privacy Rule

The Privacy Rule builds upon these existing federal regulations. The requirements are intended to strike a balance by minimizing the privacy risks of research participants, while not impeding the conduct of vital national and international research. For research participants, this means that they will have more information about how their protected health information may be used for research purposes. The Privacy Rule requires researchers who are subject to the Common Rule or FDA's human subject protection regulations to make some changes to the way they use and disclose protected health information. Researchers who are not currently subject to these requirements may, however, need to make more significant changes to current practice.

The Privacy Rule at §§ 164.508 and 164.512(i) establishes the conditions under which covered entities may disclose protected health information for research purposes. In general, covered entities are permitted to use or disclose protected health information for research either with individual authorization, or without individual authorization in limited circumstances and under certain conditions.

A covered entity is permitted to use and disclose protected health information for research purposes with an authorization from the research participant that meets the requirements of § 164.508 of the Privacy Rule. Additional requirements apply to research that is not solely record-based but, rather, involves the treatment of individuals. Specifically, in order for a covered entity to use or disclose protected health information that it creates from a research study that includes treatment of individuals (e.g., a clinical trial), the Privacy Rule at § 164.508(f) requires that additional research-specific elements be included in the authorization form, which describes how protected health information created for the research study will be used or disclosed. The Privacy Rule provides that such an authorization pursuant to § 164.508(f) may be combined with the traditional informed consent document used in research, as well as the consent required under § 164.506 and the notice of privacy practices required under § 164.520. In addition, a covered entity is permitted to condition the provision of the research-related treatment on the individual's authorization for the covered entity to use and disclose protected health information created from the study. The Privacy Rule, however, does not permit an individual authorization form for a research use or disclosure of *existing* protected health information to be combined with a research informed consent document or an authorization form for research that involves treatment.

Alternatively, a covered entity is permitted to use or disclose protected health information for research purposes without authorization by the research participant if the covered entity first obtains either of the following:

- Documentation of approval of a waiver of authorization from an IRB or a Privacy Board. The Privacy Rule delineates specific requirements for the elements that must be documented, including the Board's determinations with respect to eight defined waiver criteria.
- Where a review is conducted preparatory to research or where research is conducted on decedent's information, certain representations from the researcher, including that the use or disclosure is sought solely for such a purpose and that the protected health information is necessary for the purpose.

Public Comment

A number of commenters argued that the waiver criteria in the Privacy Rule were confusing, redundant, and internally inconsistent. These commenters urged the Department to simplify the provisions, especially for entities subject to both the Privacy Rule and the Common Rule. Consequently, these commenters recommended that the Privacy Rule be modified to allow protected health information to be used or disclosed for research without individual authorization if informed consent is obtained as stipulated by the Common Rule or FDA's human subject protection regulations, or waived as

stipulated by the Common Rule. Commenters who favored these changes asserted that the existing federal human subject protection regulations adequately protect all of the rights and welfare of human subjects, and therefore, the Privacy Rule's provisions are unnecessary and duplicative for research currently governed by federal regulations. These commenters also argued that the Privacy Rule's waiver criteria and requirements for individual authorization, in effect, inappropriately modify the Common Rule, since the Privacy Rule prohibits covered entities from honoring an IRB's decisions unless the Privacy Rule's requirements are met. Some of these commenters further suggested that the confidentiality provisions of the Common Rule and FDA's human subject protection regulations be reviewed to determine if they adequately protect the privacy of research participants, and if found to be inadequate, these regulations should be modified.

The Department understands commenters' recommendations to simplify the Privacy Rule as it applies to research. However, as stated in the preamble to the Privacy Rule and the Department's July 6 guidance, the Department disagrees that the Privacy Rule will modify the Common Rule. The Privacy Rule regulates only the content and conditions of the documentation that covered entities must obtain before using or disclosing protected health information for research purposes.

The NCVHS also heard a number of concerns and confusion in testimony at the August 2001 hearing regarding the research provisions in the Privacy Rule. As a result, the NCVHS generally recommended that the Department provide additional guidance in this area. Consistent with this recommendation, the HHS Office for Civil Rights and the HHS Office for Human Research Protections intend to work together to provide interpretations, guidance, and technical assistance to help the research community in understanding the relationship between the Privacy Rule and the Common Rule.

The NCVHS also received testimony requesting that uses and disclosures of protected health information for research be characterized as an element of treatment, payment, and health care operations under the Privacy Rule, and thus be permitted without individual authorization. The NCVHS, in their recommendations to the Department, disagreed with this viewpoint, and expressed support for the policy embodied in the Privacy Rule, permitting uses and disclosures for research pursuant to an authorization or an IRB or Privacy Board waiver of authorization.

In addition, the NCVHS received testimony regarding the issue of recruiting research subjects. Commenters expressed concern and confusion as to how researchers would be able to recruit research subjects when the Privacy Rule does not permit protected health information to be removed from the covered entity's premises during reviews preparatory to research. The NCVHS recommended that the Department provide guidance on this issue. The Department clarifies that the Privacy Rule's provisions for IRB or Privacy Board waiver of authorization are intended to encompass a partial waiver of authorization for the purposes of allowing a researcher to obtain protected health information necessary to recruit potential research participants. For example, even if an IRB does not waive informed consent and individual authorization for the study itself, it may waive such authorization to permit the disclosure of protected health information to a researcher as necessary for the researcher to be able to contact and recruit individuals as potential research subjects.

Many researchers also expressed concerns that the Privacy Rule's de-identification safe harbor was so strict that it would result in more research being subject to IRB review than is currently the case. These commenters requested that the standards for de-identification be changed in order to make de-identification a more plausible option for the sharing of data with researchers.

The Privacy Rule's de-identification safe harbor was not designed to be used for research purposes. Rather, the Privacy Rule permits uses and disclosures of protected health information for research purposes with individual authorization, or pursuant to an IRB or Privacy Board waiver of authorization as permitted by § 164.512(i). The Department is aware, however, that some research is conducted today without IRB oversight because the information is not facially identifiable. While the Department is not convinced of the need to modify the safe harbor standard for de-identified information, the Department is requesting comment on an alternative approach that would permit uses and disclosures of a limited data set for research purposes which does not include facially identifiable information but in which certain identifiers remain. See section III.I of the preamble regarding de-identification of protected health information for a detailed discussion of this proposed approach.

A number of commenters were concerned about the Privacy Rule's requirement for ''a statement of the individual's right to revoke the authorization in writing and the exceptions to the right to revoke * * *'', because this provision would prohibit researchers from analyzing the data collected prior to the individual's decision to revoke his or her authorization. The Department is not proposing to modify this provision. The Privacy Rule limits an individual's right to revoke his or her authorization by the extent to which the covered entity has taken action in reliance on the authorization. Therefore, even though a revocation will prohibit a covered entity from further disclosing protected health information for research purposes, the exception to this requirement is intended to allow for certain continued uses of the information as appropriate to preserve the integrity of the research study, *e.g.,* as necessary to account for the individual's withdrawal from the study.

The Department believes that researchers have established practices for accommodating an individual's decision to withdraw from a research study. Indeed, the Common Rule at § ___.46.116 and FDA's human subject protection regulations at 21 CFR 50.25(a)(8) contain similar provisions that require the informed consent document include a statement that ''* * * the subject may discontinue participation at any time without penalty or loss of benefits to which the subject is otherwise entitled.'' However, the Department understands that these practices may not be uniform and may vary depending on the nature of the research being conducted, with respect to the continued use or disclosure of data collected prior to the participant's withdrawal. If covered entities were permitted to continue using or disclosing protected health information for the research project even after an individual had revoked his or her authorization, this would undermine the primary objective of the authorization requirements to be a voluntary, informed choice of the individual. The Department believes that limiting uses and disclosures following revocation of an authorization to those necessary to preserve the integrity of the research appropriately balances the individual's right of choice and the researcher's reliance on the authorization. However, the Department solicits comment on other means of achieving this balance.

Specific comments, including testimony to the NCVHS, are addressed below where relevant to the corresponding proposed modifications to the Privacy Rule.

Proposed Modifications to Waiver Criteria

The Department understands commenters' concerns that several of the Privacy Rule's criteria for the waiver of a research participant's authorization are confusing and redundant, or inconsistent and conflicting with the Common Rule's requirements for the waiver of an individual's informed consent. However, since the Common Rule's criteria for the waiver of informed consent do not explicitly require IRBs to consider issues related to the privacy of prospective research participants, the Department disagrees with the recommendation to exempt from the Privacy Rule research uses and disclosures that are made with a waiver of informed consent pursuant to the Common Rule.

In response to commenter concerns, the Department proposes the following modifications to the waiver criteria to maintain uniform standards in the Privacy Rule for all research, whether or not the research is subject to the Common Rule, as well as to ensure that the Privacy Rule's waiver process works more seamlessly with the Common Rule's waiver process. The Department, in reassessing the waiver criteria defined by the Common Rule, believes that only two of the Common Rule waiver criteria are practicable when focused solely on patient privacy. Accordingly, the Department proposes to retain the following two criteria in the Privacy Rule that are comparable to two of the Common Rule criteria: (1) The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals; and (2) the research could not practicably be conducted without the waiver or alteration. The criterion in the Common Rule to determine that the rights and welfare of subjects will not adversely be affected, when limited to privacy, seems to conflict with the criterion regarding assessing minimal privacy risk; it is not clear how both criteria can be met when the focus is solely on privacy. The Department therefore proposes to delete the criterion in the Privacy Rule that the alteration or waiver will not adversely affect the privacy rights and the welfare of the individuals.

Moreover, the Department understands commenters' concerns that substantial overlap and potential inconsistency may exist among three of the Privacy Rule's criteria and the criterion that the use or disclosure involves no more than a minimal risk to the individuals. The Department believes that the three criteria in the Privacy Rule that focus on (1) plans to protect identifiers from improper use and disclosure, (2) plans to destroy the identifiers at the earliest opportunity, and (3) adequate written assurances against redisclosure, essentially help to define when the research use or disclosure poses only a minimal risk to the individual's privacy interests, rather than operate as stand-alone criteria. As such, the Department proposes to require the assessment of these three factors as part of the waiver criterion for assessment of minimal privacy risk. This provision does not preclude the IRB or Privacy Board from assessing other criteria as necessary to determine minimal privacy risk, *e.g.,* whether the safeguards included in the protocol are appropriate to the sensitivity of the data.

In addition, the Department agrees with commenters that the following waiver criterion is unnecessarily duplicative of other provisions to protect patients' confidentiality interests, and therefore, proposes to eliminate it: the privacy risks to individuals whose protected health information is to be used or disclosed are reasonable in relation to the anticipated benefits, if any, to the individual, and the importance of the knowledge that may reasonably be expected to result from the research.

Lastly, the Department proposes to retain the criterion that the research could not practicably be conducted without access to and use of the protected health information. The Privacy Rule permits a covered entity to reasonably rely on a researcher's documentation of approval of these waiver criteria, and a description of the data needed for the research as approved by an IRB or Privacy Board, to satisfy it's obligation with respect to limiting the disclosure to the minimum necessary.

In sum, the Department proposes that the following wavier criteria replace the waiver criteria listed in the Privacy Rule at § 164.512(i)(2)(ii):

(1) The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements:

(a) an adequate plan to protect the identifiers from improper use and disclosure;

(b) an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and

(c) adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of protected health information would be permitted by this subpart;

(2) The research could not practicably be conducted without the waiver or alteration; and

(3) The research could not practicably be conducted without access to and use of the protected health information.

The Department believes that the proposed modifications to the waiver criteria in the Privacy Rule would eliminate both the redundancies in the waiver criteria and the conflicts these provisions pose to research conducted pursuant to the Common Rule.

2. Research Authorizations

Several commenters argued that certain authorization requirements in the Privacy Rule at § 164.508 are problematic as applied to research uses and disclosures. Generally, commenters raised concerns that the requirements for individual authorization for uses and disclosures for research purposes are unduly complex and burdensome. In response to these concerns, the Department proposes to make a number of modifications to simplify the authorization requirements, both generally and in certain circumstances as they specifically apply to uses and disclosures of protected health information for research. The discussion below focuses on the proposed modifications specific to uses and disclosures for research. See section III.H of the preamble for a discussion of the Department's general proposal to modify the Privacy Rule's authorization requirements.

In particular, the Department proposes a single set of requirements that generally apply to all types of authorizations, including those for research purposes. This modification would eliminate the specific provisions at § 164.508(f) for authorizations for uses and disclosures of protected health information created for research that includes treatment of the individual. As a result, an authorization for such purposes would not require any additional elements above and beyond those required for authorizations in general at § 164.508(c). To conform to this proposed change, the Department also proposes to modify the requirements for prohibiting

conditioning of authorizations at § 164.508(b)(4)(i) to remove the reference to § 164.508(f). A covered health care provider, thus, would be able to condition the provision of research-related treatment on provision of an authorization for the use and disclosure of protected health information for the particular research study.

Additionally, the Department proposes to modify § 164.508(b)(3)(i) to reflect its intent to eliminate the special authorization requirements for research studies that involve treatment in § 164.508(f), as well as to clarify that the Privacy Rule would allow an authorization for the use or disclosure of protected health information for research to be combined with any other legal permission related to the research study, including another authorization or consent to participate in the research. The Department heard from several provider groups who thought the authorization provisions as they relate to research to be too complex. These commenters argued in favor of permitting covered entities to combine all of the research authorizations required by the Privacy Rule with the informed consent to participate in research. To simplify the requirements in response to these concerns, the Department proposes to modify the Privacy Rule to allow for the combining of such permissions.

Finally, the Department proposes to include provisions specific to authorizations for research within the core element proposed at § 164.508(c)(1)(v) for an expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. First, the Department proposes to explicitly provide that the statement ''end of the research study'' or similar language is sufficient to meet this requirement for an expiration date or event where the authorization is for a use or disclosure of protected health information for research. This modification is proposed in response to commenter concerns that the particular end date of a research study may not be known and questions regarding whether the end of a research study is an ''event''. In addition, such a statement would also be sufficient to encompass additional time, even after the conclusion of the research, to allow for the use of protected health information as necessary to meet record retention requirements to which the researcher is subject. The Department, therefore, proposes to clarify that including such a statement on the research authorization would fulfill the requirement to include an expiration event.

Similarly, the Department proposes to explicitly provide that the statement ''none'' or similar language is sufficient to meet this provision if the authorization is for a covered entity to use or disclose protected health information for the creation or maintenance of a research database or repository. The Department proposes this modification in response to commenter concerns that the Privacy Rule's requirement for an ''expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure'' will create a significant obstacle for the development of research databases or repositories. Commenters stated that research databases and repositories are often retained indefinitely, and the requirement that an authorization include an expiration date or event was found to be counter to the purpose of developing such research resources. The Department understands these concerns and, therefore, proposes to permit an individual's authorization to use or disclose protected health information for the creation and maintenance of a research database or repository to be valid without an expiration date or event. The Department emphasizes that this provision is intended to apply only in the limited circumstances where a use or disclosure is sought solely for the creation or maintenance of a database or repository, and does not extend to authorizations for further research or any other purpose. Therefore, subsequent research using the information maintained in the database or repository pursuant to an authorization would require that the authorization include the term ''end of the research study'' or other explicit expiration date or event.

3. Research Transition Provisions

The Privacy Rule includes at § 164.532 different transition requirements for research that includes treatment (*i.e.,* clinical trials) and for research that does not include treatment (*i.e.,* records research). For research that includes treatment, the Privacy Rule states that as long as legal permission was obtained to use or disclose protected health information for a specific research project, that legal permission will continue to be valid until the completion of the research project; a new permission will not be required to use or disclose protected health information that was created or received either before or after the compliance date. However, for research that does not include treatment, a legal permission obtained before the compliance date will only be valid for the use and disclosure of protected health information obtained before the compliance date. The Privacy Rule does not prescribe the form of the express legal permission in either case. Express legal permission could be a signed agreement by the individual to participate in a privately-funded research study.

The Privacy Rule does not explicitly address transition provisions for research studies ongoing after the compliance date where the legal permission of the individual had not been sought. This point was noted by several of those who commented on the Privacy Rule's transition provisions as they apply to research. Some of these commenters recommended that the Privacy Rule be revised to grandfather in the research use and disclosure of all protected health information that existed prior to the compliance date. These commenters expressed concern that much data would be lost to the research community since it would often be infeasible or impossible to obtain individuals' permission to use this archival information.

Given the confusion about the transition provisions and to assure that ongoing, vital research will not be impeded, the Department reassessed the relevant provisions and proposes that there be no distinction between research that includes treatment and research that does not, and no distinction between requirements for research conducted with patients' informed consent versus research conducted with an IRB-approved waiver of patients' informed consent. Therefore, the Department proposes to permit a covered entity to use or disclose for a specific research study protected health information that is created or received either before or after the compliance date (if there is no agreed-to restriction in accordance with § 164.522(a)), if the covered entity has obtained, prior to the compliance date an authorization or other express legal permission from an individual to use or disclose protected health information for the research study. In addition, the Department proposes to grandfather in research in which the individual has signed an informed consent to participate in the research study, or an IRB has waived informed consent for the research study, in accordance with the Common Rule or FDA's human subject protection regulations.

These proposed provisions are intended to apply once any of the permissions described above has been granted, regardless of whether the

research study actually has begun by the compliance date or not, provided that the permission was obtained prior to the compliance date. In addition, with respect to the informed consent of the individual, the Department proposes not to limit the transition provisions to an informed consent pursuant to the Common Rule, but rather intends to allow for the transition of an informed consent for privately-funded research. Research studies that do not obtain such express legal permission, informed consent, or IRB waiver prior to the compliance date must obtain either authorization, as required by § 164.508, or a waiver of authorization from an IRB or Privacy Board, as required by § 164.512(i).

H. Uses and Disclosures for Which Authorization Is Required

The Privacy Rule permits covered entities to use and disclose protected health information for treatment, payment, and health care operations (subject to the individual's consent, if applicable) and as necessary for public policy purposes, such as public health and safety, health oversight activities, and enforcement. Covered entities must obtain an individual's voluntary and informed authorization before using or disclosing protected health information for any purpose that is not otherwise permitted or required under the Privacy Rule.

The Privacy Rule provides for the individual's voluntary authorization for uses and disclosure of his or her protected health information by prohibiting, with very limited exceptions, covered entities from conditioning treatment, payment, or eligibility for benefits or enrollment in a health plan, on obtaining an authorization. Furthermore, in § 164.508(b)(5), the Privacy Rule permits individuals, with limited exceptions, to revoke an authorization at any time. These provisions are intended to prevent covered entities from coercing individuals into signing an authorization that is not necessary for their health care.

To help ensure that individuals give their authorization for the use or disclosure of their protected health information on an informed basis, the Privacy Rule, under § 164.508(c), sets out core elements that must be included in any authorization. These core elements are intended to provide individuals with information needed to make an informed decision about giving their authorization. This information includes specific details about the use or disclosure, as well as providing the individual fair notice about his or her rights with respect to the authorization and the potential for the information to be redisclosed. The Privacy Rule requires authorizations to provide individuals with additional information for specific circumstances under the following three sets of implementation specifications: in § 164.508(d), for authorizations requested by a covered entity for its own uses and disclosures; in § 164.508(e), for authorizations requested by a covered entity for disclosures by others; and in § 164.508(f), for authorizations for research that includes treatment of the individual. Additionally, the authorization must be written in plain language so individuals can understand the information presented in the authorization.

Public Comments

The Department received a number of comments raising various issues regarding implementation of the authorization requirements. A majority of commenters said the authorization provisions of the Privacy Rule are too complex and confusing. Some commented that the sets of implementation specifications are not discrete, creating the potential for the implementation specifications for specific circumstances to conflict with the required core elements. Others expressed confusion generally about which authorization requirements they would be required to implement.

Commenters also have raised concerns about the revocation provisions in § 164.508(b)(5). The Privacy Rule provides an exception to the individual's right to revoke an authorization where the authorization is obtained as a condition of obtaining insurance coverage, or where other law provides the insurer the right to contest a claim under the policy. The Department intended this provision to permit insurers to obtain necessary protected health information during contestability periods under State law. For example, an individual may not revoke an authorization for the disclosure of protected health information to a life insurer for the purpose of investigating material misrepresentation if the individual's policy is still subject to the contestability period. However, commenters were concerned because other law also provides the insurer with the right to contest the policy itself, not just a claim under the policy, and the Privacy Rule does not provide an explicit exception to allow for this right.

Proposed Modifications

In response to these concerns, the Department is proposing modifications to the Privacy Rule to simplify the authorization provisions, while preserving the provisions for ensuring that authorizing the use or disclosure of protected health information is a voluntary and informed decision. The Department proposes to consolidate the implementation specifications into a single set of criteria to simplify these provisions, prevent confusion, and eliminate the potential for conflicts between the authorization requirements.

Thus, under the proposed modifications, the specifications for the elements and requirements of an authorization would be consolidated under § 164.508(c). Paragraphs (d), (e), and (f) in this section would be eliminated. Paragraph (c)(1) would require all authorizations to contain the following core elements: (1) A description of the information to be used or disclosed, (2) the identification of the persons or class of persons authorized to make the use or disclosure of the protected health information, (3) the identification of the persons or class of persons to whom the covered entity is authorized to make the use or disclosure, (4) a description of each purpose of the use or disclosure, (5) an expiration date or event, (6) the individual's signature and date, and (7) if signed by a personal representative, a description of his or her authority to act for the individual. The Department also proposes to add new language to clarify that when the individual initiates the authorization for his or her own purposes, the purpose may be described as ''at the request of the individual.'' Thus, individuals would not have to reveal the purpose of the requested disclosure if they chose not to do so.

Paragraph (c)(2) would require authorizations to contain the following notifications: (1) A statement that the individual may revoke the authorization in writing, and either a statement regarding the right to revoke, and instructions on how to exercise such right, or to the extent this information is included in the covered entity's notice, a reference to the notice, (2) a statement that treatment, payment, enrollment, or eligibility for benefits may not be conditioned on obtaining the authorization if such conditioning is prohibited by the Privacy Rule, or, if conditioning is permitted by the Privacy Rule, a statement about the consequences of refusing to sign the authorization, and (3) a statement about the potential for the protected health information to be subject to redisclosure

by the recipient. The Department also proposes to limit the requirement that a covered entity disclose any remuneration that will result from obtaining an authorization, to authorizations for marketing purposes. Therefore, the remuneration disclosure requirement appears only in the new § 164.508(a)(3) on marketing authorizations. These modifications would permit covered entities to use a single authorization form, and make it easier to use for the individual and the covered entity, as well as third parties.

The Department also proposes to add language to the revocation exceptions in § 164.508(b)(5)(ii) to include an exception with respect to the insurer's right to contest the policy under other law. This proposed modification would recognize, without expanding upon, an insurer's right to contest the policy under existing law.

Other proposed modifications concerning authorizations for research are discussed in section III.G of the preamble.

Finally, the Department proposes a number of technical conforming modifications throughout this section of the Privacy Rule to accommodate the modifications to this section, as well as the proposed modifications to the consent provision. Specifically, the Department proposes to modify the exception to the minimum necessary standard in the Privacy Rule at § 164.502(b)(2), which exempts from the standard uses or disclosures made pursuant to an authorization under § 164.508, except for authorizations requested by the covered entity under § 164.508(d), (e), or (f). By simplifying the authorization requirements, the proposed modifications described above would eliminate the special authorizations required by § 164.508(d), (e), or (f) in the Privacy Rule. To be consistent with the proposed approach, the Department proposes to eliminate the reference to such authorizations in the exception at § 164.502(b)(2), thereby expanding the exception to exempt from the minimum necessary standard uses and disclosures made pursuant to an authorization for any purpose.

The Department also proposes modifications at §§ 164.508(a)(2)(i)(A), (B), and (C) to place limits on the use and disclosure of psychotherapy notes without authorization to carry out treatment, payment or health care operations. The modifications clarify that this information is not permitted to be used or disclosed without individual authorization for purposes of another entity.

The Department proposes to delete § 164.508(b)(4)(iii), relating to a health plan conditioning payment of a claim on the provision of an authorization, since this provision will be rendered moot under the proposed modifications to the consent provision. Additionally, the Department proposes to delete § 164.508(b)(2)(iv) of the Privacy Rule, because it is redundant with § 164.508(b)(1)(i), and to modify § 164.508(b)(1)(i) to clarify that an authorization is valid only if it meets the requirements of paragraphs (c)(1) and (c)(2). Modifications are also proposed at § 164.508(b)(1)(v) of the Privacy Rule (newly designated as § 164.508(b)(2)(iv) in the proposed Rule) to clarify that an authorization that violates paragraph (b)(4) (prohibiting the conditioning of authorizations) is not a valid authorization.

These proposed modifications also expressly provide that an authorization is needed for purposes of marketing. *See* section III.G of the preamble for a detailed discussion of the proposed modifications regarding marketing.

I. De-Identification of Protected Health Information

At § 164.514(a)–(c), the Privacy Rule permits a covered entity to de-identify protected health information so that such information may be used and disclosed freely, without being subject to the Privacy Rule's protections. Health information is de-identified, or not individually identifiable, under the Privacy Rule, if it does not identify an individual and if the covered entity has no reasonable basis to believe that the information can be used to identify an individual. In order to meet this standard, the Privacy Rule provides two alternative methods for covered entities to de-identify protected health information.

First, a covered entity may demonstrate that it has met the standard if a person with appropriate knowledge and experience applying generally acceptable statistical and scientific principles and methods for rendering information not individually identifiable makes and documents a determination that there is a very small risk that the information could be used by others to identify a subject of the information. The preamble to the Privacy Rule refers to two government reports that provide guidance for applying these principles and methods, including describing types of techniques intended to reduce the risk of disclosure that should be considered by a professional when de-identifying health information. These techniques include removing all direct identifiers, reducing the number of variables on which a match might be made, and limiting the distribution of records through a ''data use agreement'' or ''restricted access agreement'' in which the recipient agrees to limits on who can use or receive the data.

Alternatively, covered entities may choose to use the Privacy Rule's safe harbor method for de-identification. Under the safe harbor method, covered entities must remove all of a list of 18 enumerated identifiers and have no actual knowledge that the information remaining could be used alone or in combination to identify a subject of the information. The identifiers that must be removed include direct identifiers, such as name, street address, social security number, as well as other identifiers, such as birth date, admission and discharge dates, and five-digit zip code. The safe harbor does allow for the disclosure of all geographic subdivisions no smaller than a State, as well as the initial three digits of a zip code if the geographic unit formed by combining all zip codes with the same initial three digits contains more than 20,000 people. In addition, age, if less than 90, gender, ethnicity, and other demographic information not listed may remain in the information. The safe harbor is intended to provide covered entities with a simple, definitive method that does not require much judgment by the covered entity to determine if the information is adequately de-identified.

The Privacy Rule also allows for the covered entity to assign a code or other means of record identification to allow de-identified information to be re-identified by the covered entity, if the code is not derived from or related to information about the subject of the information, *e.g.,* derivation of the individual's social security number, and is not otherwise capable of being translated so as to identify the individual. The covered entity also may not use or disclose the code for any other purpose, and may not disclose the mechanism, *e.g.,* algorithm or other tool, for re-identification.

The Department is cognizant of the increasing capabilities and sophistication of electronic data matching used to link data elements from various sources, and from which, therefore, individuals may be identified. Given this increasing risk to individuals' privacy, the Department included in the Privacy Rule the above stringent standards for determining when information may flow unprotected. The Department also wanted the standards to be flexible enough so the Privacy Rule would not be a disincentive for covered entities to use or disclose de-identified

information wherever possible. The Privacy Rule, therefore, strives to balance an individuals' privacy interests with providing a sufficient level of information to make de-identified databases useful.

Public Comments

The Department heard a number of concerns from commenters regarding the de-identification standard in the Privacy Rule. These comments generally were raised in the context of using and disclosing information for research, public health purposes, or for certain health care operations. Commenters were concerned that the safe harbor method for de-identifying protected health information was so stringent that it required removal of many of the data elements that were essential to their analyses for these purposes. The comments, however, demonstrated little consensus as to which data elements were needed for such analyses, with many commenters requesting elements, such as birth date, neighborhood, account numbers, medical record numbers, and device identifiers. In addition, commenters largely were silent with regard to the feasibility of using the Privacy Rule's alternative statistical method to de-identify information. The Department is aware, however, of a general view of covered entities that the statistical method is beyond their capabilities.

With regard to health care operations, a number of state hospital associations were concerned that the Privacy Rule will prevent them from collecting patient information from area hospitals in order to conduct and disseminate analyses that are useful for hospitals in making decisions about quality and efficiency improvements. These commenters explained that the Privacy Rule's stringent provisions for de-identification would not allow for the necessary data elements to be collected for such analyses. Specifically, commenters identified the following critical elements that would be restricted from disclosure by the Privacy Rule's de-identification standard: Five-digit zip code, city, county or neighborhood; the dates on which the injury or illness was treated and the patient released from the hospital; and the month of birth (noted by commenters as especially important for very young children). In addition, commenters argued that the Privacy Rule's provisions for data aggregation by a business associate, while allowing for the collection and aggregation of identifiable data from multiple hospitals for quality and efficiency purposes, would not allow state hospital associations to disclose all the desired analyses back to the contributing hospitals because some identifiers would remain in the data. These commenters emphasized the importance to hospitals to have access to information about community health care needs and the ability to compare their community to others in the state so that they may adequately respond to and fulfill such needs.

In addition, commenters identified a problem with hospitals themselves sharing aggregated information with other hospitals for health care operations purposes. The Privacy Rule prohibits covered entities from disclosing protected health information for the health care operations purposes of other covered entities. As described in section III.A.2 of the preamble regarding Uses and Disclosures for Treatment, Payment, and Health Care Operations, the Department is proposing to modify this restriction and allow covered entities to disclose protected health information for another covered entity's health care operations under some circumstances. However, two conditions on the sharing of individually identifiable information for health care operations may continue to pose a problem. The proposed modifications would condition the sharing on both entities being covered entities and both entities having a relationship with the individual. Hospitals wishing to exchange patient information with each other or with other community health care providers would not satisfy these conditions in all cases.

Many researchers expressed similar concerns, explaining that the Privacy Rule's de-identification safe harbor was so strict that it would result in more research being done on identifiable health information and, thereby, being subject to IRB review than is currently the case. Under the Common Rule, research that uses ''identifiable private information'' must undergo IRB review. However, there is no agreed-upon definition of ''identifiable private information'' and IRBs determine on a case-by-case basis what constitutes ''identifiable private information.'' Consistent with this variability, the comments did not demonstrate consensus on what identifiers should be permitted to be retained for research purposes.

In addition, commenters also expressed concerns with respect to public health reporting. For example, some product manufacturers subject to the jurisdiction of FDA were concerned that they would not be able to operate post-marketing surveillance registries, to which health care providers report problems. Commenters stated that even though they do not need information with direct identifiers, the Privacy Rule's strict de-identification standard would not allow the reporting of useful information into the registry. Additionally, a number of commenters described the de-identification standard as hampering many research and health care operations activities that also serve a public health purpose, *e.g.,* the tracking of the emergence of disease that could be the result of bioterrorism.

The Department also heard from some consumer advocates who supported the elimination of barriers they believe are imposed by the de-identification standard to important medical research. In order to ensure privacy is protected, but at the same time not render impossible research using de-identified information, these commenters recommended that the Department permit the use of information for research that is facially de-identified, *i.e.,* stripped of direct identifiers, so long as the research entity provides assurances that it will not use or disclose the information for purposes other than research and will not identify or contact the individuals who are the subjects of the information.

Solicitation of Comment

The Department is aware of the importance of the activities described by the commenters but is not currently convinced of the need to modify the safe harbor standard for de-identified information. Instead, the Department requests comment on an alternative approach that would permit uses and disclosures of a limited data set which does not include facially identifiable information but in which certain identifiers would remain. The Department is not considering permitting the disclosure of any such limited data set for general purposes, but rather is considering permitting disclosure of such information for research, public health, and health care operations purposes.

The limited data set would not include the following information, which the Department considers direct identifiers: name, street address, telephone and fax numbers, e-mail address, social security number, certificate/license number, vehicle identifiers and serial numbers, URLs and IP addresses, and full face photos and any other comparable images. The limited data set would include the following identifiable information: admission, discharge, and service dates; date of death; age (including age 90 or over); and five-digit zip code. The

Department solicits comment on whether another one or more geographic units smaller than State, such as city, county, precinct, neighborhood or other unit, would be needed in addition to, or be preferable to, five-digit zip code.

In addition, to address concerns raised by commenters regarding access to birth date for research or other studies relating to young children or infants, the Department clarifies that the Privacy Rule does not prohibit age of an individual from being expressed as an age in months, days, or hours. Given that the limited data set would include all ages, including age in months, days, or hours, if preferable, the Department requests comment on whether date of birth is needed and, if so, whether the entire date is needed, or just the month and year.

In addition, to further protect privacy, the Department would propose to condition the disclosure of the limited data set on covered entities obtaining from the recipients a data use or similar agreement, in which the recipient would agree to limit the use of the limited data set to the specified purposes in the Privacy Rule, and limit who can use or receive the data, as well as agree not to re-identify the data or contact the individuals. Commenters seemed to indicate that recipients would be amenable to such conditions.

The Department solicits public comment on the feasibility and acceptability of the above approach for the described purposes, and whether or not the limitations and conditions would be sufficiently protective of patient privacy.

Proposed Modifications

In addition to the solicitation of comment above, the Department proposes a technical modification to the safe harbor provisions. A number of commenters expressed confusion regarding what was believed to be conflicting provisions within the de-identification standard. Commenters argued that, on the one hand, the Privacy Rule treats information as de-identified if all listed identifiers on the information are stripped, including any unique, identifying number, characteristic, or code. Yet, the Privacy Rule permits a covered entity to assign a code or other record identification to the information so that it may be re-identified by the covered entity at some later date.

The Department did not intend the re-identification code to be considered one of the enumerated identifiers. Therefore, the Department proposes to clarify its intent by explicitly excepting the re-identification code or other means of record identification permitted by § 164.514(c) from the listed identifiers at § 164.514(b)(2)(i)(R).

J. Technical Corrections and Other Clarifications

In addition to the modifications described above, the Department proposes to make the following clarifications:

1. Changes of Legal Ownership. The Privacy Rule's definition of health care operations, at §164.501, includes business management and general administrative activities of the entity, including, due diligence in connection with the sale or transfer of assets to a potential successor in interest, if the potential successor in interest is a covered entity or, following completion of the sale or transfer, will become a covered entity.

In the preamble to the Privacy Rule, the Department explained that this language was included to remedy an omission in the 1999 proposed Rule by

> add[ing] to the definition of health care operations disclosures of protected health information for due diligence to a covered entity that is a potential successor in interest. This provision includes disclosures pursuant to the sale of a covered entity's business as a going concern, mergers, acquisitions, consolidations, and other similar types of corporate restructuring between covered entities, including a division of a covered entity, and to an entity that is not a covered entity but will become a covered entity if the reorganization or sale is completed.

65 FR at 82609 (December 28, 2000) (response to comment); *see also* 65 FR at 82491 (similar language); 65 FR at 82652 (''We clarify in the definition of health care operations that a covered entity may sell or transfer its assets, including protected health information, to a successor in interest that is or will become a covered entity.'')

Despite language in the preamble to the contrary, the definition of health care operations in the Privacy Rule does not expressly provide for the transfer of protected health information upon sale or transfer to a successor in interest. Instead, the definition of ''health care operations'' only mentions disclosures of protected health information for ''due diligence'' purposes when a sale or transfer to a successor in interest is contemplated. ''Due diligence'' is generally understood to mean the ''[a] prospective buyer's or broker's investigation and analysis of a target company, a piece of property, or a newly issued security.'' Black's Law Dictionary (7th ed. 1999) *available in* Westlaw, DIBLACK database.

The Department proposes to add language to paragraph (6) of the definition of ''health care operations'' to clarify the intent to permit the transfer of records to a covered entity upon a sale, transfer, merger, or consolidation. This proposed change would prevent the Privacy Rule from interfering with necessary treatment or payment activities upon the sale of a covered entity or its assets.

The Department also proposes to use the terms ''sale, transfer, consolidation or merger'' to eliminate the term ''successor in interest'' from this paragraph. The Department intended this provision to apply to any sale, transfer, merger or consolidation and believes the current language may not sufficiently accomplish this goal. The proposed language's use of the terms ''sale, transfer, merger and consolidation'' is based on language used in model State laws addressing the disclosure of personal or privileged information collected or received in connection with an insurance transaction.

The Department retains the limitation that such disclosures are health care operations only to the extent the entity receiving the protected health information is a covered entity or will become a covered entity as a result of the sale, transfer, merger, or consolidation. In addition, the proposed modification does not affect any responsibility of covered entities either under other law or ethical obligation to notify individuals appropriately of a sale, transfer, merger, or consolidation.

2. Group Health Plan Disclosures of Enrollment and Disenrollment Information to Plan Sponsors. The Department proposes to modify the Privacy Rule to make express the Department's policy, which was explained in the preamble to the Privacy Rule, that group health plans are permitted to share enrollment and disenrollment information with plan sponsors without amending plan documents. Under the Privacy Rule, a group health plan, as well as a health insurance issuer or HMO providing health insurance or health coverage to the group health plan, are covered entities. Neither employers nor other plan sponsors are defined as covered entities. The Department recognizes the legitimate need of the plan sponsor to have access to health information of these covered entities in certain situations. Therefore, the Privacy Rule at § 164.504(f) permits a group health plan, and health insurance issuers or HMOs with respect to the group health plan, to disclose protected health information to the plan sponsor provided that, among other requirements, the plan documents are

amended to appropriately reflect and restrict the plan sponsor's uses and disclosures of such information.

There are two exceptions where the Privacy Rule permits group health plans (or health insurance issuers or HMOs, as appropriate) to disclose information to a plan sponsor without requiring amendment of plan documents. First, § 164.504(f) permits such disclosures when the information needed by the plan sponsor is summary health information. Second, as explained in the preamble to the Privacy Rule, a plan sponsor is permitted to perform enrollment functions on behalf of its employees without meeting the requirements of § 164.504(f), as such functions are considered outside of the plan administration functions. Therefore, a group health plan is also permitted to disclose enrollment or disenrollment information to the plan sponsor without amending the plan documents as required by § 164.504(f).

However, this policy regarding disclosures of enrollment or disenrollment information was addressed only in the preamble to the Privacy Rule and not explicitly in the regulation itself. As a result, the policy seems to have been overlooked and the absence of a specific provision in the regulation itself has caused misinterpretation within industry. To remedy this misunderstanding and make its policy clear, the Department proposes to add an explicit exception at § 164.504(f)(1)(iii) to clarify that group health plans (or health insurance issuers or HMOs, as appropriate) are permitted to disclose enrollment or disenrollment information to a plan sponsor without meeting the plan document amendment and other related requirements.

3. Definition of ''Individually Identifiable Health Information.'' The Department proposes to move the definition of ''individually identifiable health information'' from § 164.501 to § 160.103 to clarify that the definition is relevant to all of the provisions in Parts 160 through 164.

4. Accounting of Disclosures of Protected Health Information. Under the Privacy Rule at § 164.528, individuals have the right to receive an accounting of disclosures of protected health information made by the covered entity, with certain exceptions. These exceptions, or instances where a covered entity is not required to account for disclosures, include disclosures made by the covered entity to carry out treatment, payment, or health care operations, as well as disclosures to individuals of protected health information about them.

The accounting is required to include the following: (1) disclosures of protected health information that occurred during the six years prior to the date of the request for an accounting, including disclosures to or by a business associate of the covered entity; (2) for each disclosure: the date of the disclosure; the name of the entity or person who received the protected health information; if known, the address of such entity or person; a brief description of the protected health information disclosed; and a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or in lieu of such a statement, a copy of the individual's written authorization pursuant to § 164.508 or a copy of a written request for a disclosure under §§ 164.502(a)(2)(ii) or 164.512. For multiple disclosures of protected health information to the same person, the Privacy Rule allows covered entities to provide individuals with an accounting that contains only the following information: (1) For the first disclosure, a full accounting, with the elements described in (2) above; (2) the frequency, periodicity, or number of disclosures made during the accounting period; and (3) the date of the last such disclosure made during the accounting period.

A number of commenters raised concerns that the high costs and administrative burdens associated with the accounting requirements would deter covered entities from disclosing protected health information. In response to these concerns, the Department proposes to expand the exceptions to the standard at § 164.528(a)(1) to include disclosures made pursuant to an authorization as provided in § 164.508. Covered entities would no longer be required to account for any disclosures authorized by the individual in accordance with § 164.508. The Department is proposing to alleviate burden in this way because it is believed that an accounting of disclosures made pursuant to such permissions is unnecessary because such disclosures are already known by the individual, in as much as the individual was required to sign the forms authorizing the disclosures.

Accordingly, the Department proposes to make two conforming amendments at §§ 164.528(b)(2)(iv) and (b)(3) to delete references in the accounting content requirements to disclosures made pursuant to an authorization.

5. Uses and Disclosures Regarding FDA-regulated Products and Activities. The Department recognizes the importance of public health activities and, in the Privacy Rule, allows information to be used and disclosed for these purposes without requiring individual consent or authorization. The recent anthrax attacks and the threat of other forms of bio-terrorism have served to underscore the vital necessity of a strong and effective public health system. The Rule allows covered entities to disclose protected health information to public health authorities for a broad array of public health purposes, including reporting of diseases, injuries, vital statistics, and for the conduct of public health surveillance and interventions. The Rule permits public health reporting to private persons who are contractors for or agents of the public health authority. The Rule also recognizes the essential role of manufacturers and other private persons in carrying out the Food and Drug Administration's (FDA) public health mission.

The Privacy Rule, at § 164.512(b)(1)(iii), specifically permits covered entities to disclose protected health information, without individual authorization, to a person who is subject to the jurisdiction of the FDA for the following specified purposes: (1) To report adverse events, defects or problems, or biological product deviations with respect to products regulated by the FDA (if the disclosure is made to the person required or directed to report such information to the FDA), (2) to track products (if the disclosure is made to the person required or directed to report such information to the FDA), (3) for product recalls, repairs, or replacement, and (4) for conducting post-marketing surveillance to comply with FDA requirements or at the direction of the FDA.

The Department received a number of comments on the provisions for public health activities related to FDA-regulated products. The majority of these commenters were concerned that the Privacy Rule constrains important public health surveillance and reporting activities by impeding the flow of needed information to those subject to the FDA's jurisdiction. In particular, commenters noted that limiting disclosures to those that are ''required or directed'' by FDA does not reflect the breadth of public health activities that are currently being conducted by the private sector on a voluntary basis or under the general auspices of—but not at the direction of—FDA. In general, commenters were concerned that such limitations would stifle current reporting practices. For example, the

FDA currently obtains the vast majority of its information about drugs and devices indirectly from health care providers who voluntarily report known adverse events or problems to the manufacturer of the product. The manufacturer may or may not be required to report such adverse events to FDA. Commenters assert that the present language of the Privacy Rule will have a ''chilling effect'' on these important communications due to uncertainty over the manufacturer's obligation to report to the FDA.

Some concern was expressed about the potential liability of a covered entity for a disclosure to an employee of the manufacturer who is not ''a person subject to the jurisdiction of the FDA'' or to the wrong manufacturer. The Department seeks to assure covered entities that use of the term ''a person'' was not intended to limit reporting to a single individual within an entity, but to allow reporting to flow as it does today between health care providers and representatives of manufacturers or other companies. Moreover, the Department seeks to clarify that covered entities may continue to disclose protected health information to the companies identified on the product labels as the manufacturer registered with the FDA to distribute the product.

To eliminate the ''chilling effect'' of the Rule, some commenters requested that the Department include in the Rule a ''good-faith'' safe harbor to protect covered entities from enforcement actions arising from unintentional violations of the Privacy Rule. For example, a health care provider would not have violated the Rule if the disclosure was made in the good faith belief that the entity to whom the adverse event was reported was responsible for the FDA-regulated product, even if it turned out to be the wrong manufacturer.

Finally, a number of commenters, including some that are subject to the FDA's jurisdiction, suggested that: identifiable health information is not necessary for some or all of these public health reporting purposes; that identifiable health information is not reported to FDA; and that for purposes of post-marketing surveillance, information without direct identifiers (such as name, mailing address, phone number, social security number, and email address) should suffice. The Department recognizes that there must be a balance between the need for public health activities that benefit every individual by safeguarding the effectiveness, safety, and quality of the products regulated by the FDA, and the privacy interests of specific individuals. However, the comments did not offer a consensus as to which activities could be performed without identifiable information or which identifiers, if any, were needed. In Section III.I of this preamble regarding De-identification issues, the Department is soliciting comments on a limited data set for use for specific purposes, including public health. The Department also requests comments as to whether this limited data set should be required or permitted for some or all public health purposes or if a special rule should be developed for public health reporting.

The Department did not intend the Privacy Rule to discourage or prevent the reporting of adverse events or otherwise disrupt the flow of essential information that FDA and persons subject to the jurisdiction of FDA need in order to carry out their important public health activities. Therefore, the Department proposes a number of changes to eliminate uncertainties identified by the commenters, and, thereby, encourage covered entities to continue to report and cooperate in these essential public health activities. The proposed modifications attempt to recognize and preserve current public health activities of persons subject to the jurisdiction of the FDA while not diminishing the health information privacy protections for individuals.

Specifically, the Department proposes to remove from § 164.512(b)(1)(iii)(A) and (B) the phrase ''if the disclosure is made to a person required or directed to report such information to the Food and Drug Administration'' and to remove from subparagraph (D) the phrase ''to comply with requirements or at the direction of the Food and Drug Administration.'' In lieu of this language, HHS proposes to describe at the outset the public health purposes for which disclosures may be made. The proposed language reads: ''A person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity.''

The Department proposes to retain the listing of specific activities identified in paragraphs (A), (B), (C), and (D), to give covered entities additional assurance that public health disclosures for these activities are permissible under the Privacy Rule. The listing, however, is no longer an exclusive list of FDA-related public health activities, but rather is a list of examples of the most common activities. Additionally, language has been added to paragraph (C) to include ''lookback'' activities which are necessary for tracking blood and plasma products, as well as quarantining tainted blood or plasma and notifying recipients of such tainted products.

The privacy of individuals' health information would continue to be protected through the limitations placed on the permissible disclosures for FDA purposes. Specifically, such disclosures must relate to FDA-regulated products or activities for which the person using or receiving the information has responsibility, and for activities related to the safety, effectiveness, or quality of such FDA-regulated product or activity.

The Department is not proposing a good-faith safe harbor at this time because it believes that these proposed modifications will adequately address the concerns and uncertainties facing covered entities. However, the Department is interested in hearing from affected parties as to whether the proposed modifications are adequate or if additional measures are necessary for health care providers or others to continue to report this vital information about FDA-regulated products or activities.

6. Hybrid Entities. The Privacy Rule defines covered entities that primarily engage in activities that are not covered functions—i.e., functions that relate to the entity's operation as a health plan, health care provider, or health care clearinghouse—as hybrid entities. See § 164.504(a). In order to limit the burden on such entities, most of the requirements of the Privacy Rule only apply to the health care component(s) of the hybrid entity and not to the parts of the entity that do not engage in covered functions. The health care component(s) include those components of the entity that perform covered functions and other components of the entity that support those covered functions, in the same way such support may be provided by a business associate. A covered entity that is a hybrid entity is required to define and designate those parts of the entity that engage in the covered functions and ''business associate'' functions and that are, therefore, part of the health care component(s). The health care component is designed to include components that engage in ''business associate'' functions because it is impossible for the entity to contract with itself and the authorization requirement would limit the ability to engage in necessary health care operations functions.

The hybrid entity is also required to create adequate separation (i.e., fire walls) between the health care component(s) and other components of

the entity. Transfer of protected health information held by the health care component to other components of the hybrid entity is a disclosure under the Privacy Rule and is only allowed to the same extent as such disclosure would be permitted to a separate entity.

Examples of hybrid entities are: (1) corporations that are not in the health care industry, but that operate on-site health clinics, and (2) insurance carriers that have multiple lines of business which include both health insurance and other insurance lines such as general liability or property and casualty insurance.

A ''hybrid entity'' is defined in the Privacy Rule as an entity ''whose covered functions are not its *primary* functions.'' (emphasis added). In the preamble to the Privacy Rule, the Department explained that the use of the term ''primary'' in the definition of a ''hybrid entity'' was not intended to operate with mathematical precision. The Department intended a common sense evaluation of whether the covered entity mostly operates as a health plan, health care provider, or health care clearinghouse. If an entity's primary activity was engaging in covered functions, then the whole entity would be a covered entity and the hybrid entity provisions would not apply. However, if the covered entity primarily conducted non-health activities, it would qualify as a hybrid entity and would be required to comply with the Privacy Rule with respect to its health care component(s). Commenters expressed concern that the policy guidance in the preamble was insufficient as long as the Privacy Rule itself limited the hybrid entity provisions to entities that primarily conducted non-health related activities. There were particular concerns in cases in which the health plan line of business was the primary business, and the line of business that is one of the excepted benefits, *e.g.,* workers' compensation insurance, was only a small portion of the business. There were also concerns about what ''primary'' meant if not a mathematical calculation and how the entity would know whether or not it was a hybrid entity based on the guidance in the preamble.

As a result of these comments, the Department proposes to delete the term ''primary'' from the definition of ''hybrid entity'' in § 164.504(a). In order to avoid the problem of line drawing, the Department proposes to permit any covered entity to be a hybrid entity if it is a single legal entity that performs both covered and non-covered functions, regardless of whether the non-covered functions represent that entity's primary function, a substantial function, or even a small portion of the entity's activities.

The Department proposes to permit covered entities that could qualify as hybrid entities to choose whether or not they want to be hybrid entities. Elimination of the requirement in the definition of ''hybrid entity'' that covered functions not be the ''primary'' functions of the covered entity would greatly increase the proportion of covered entities that are hybrid entities. In order to avoid the burden of requiring many more covered entities to designate the health care components and create fire walls within their entity when it is administratively simpler to treat the entire entity as a covered entity, the proposal would allow the covered entity to choose whether it will be a hybrid entity or not. To accomplish this objective, the proposed definition of ''hybrid entity'' would require that in order to be a hybrid entity, a covered entity that otherwise qualifies must designate health care components. If a covered entity does not designate health care components, the entire entity would be a covered entity.

There are advantages and disadvantages to being a hybrid entity. Whether or not the advantages outweigh the disadvantages will be a decision of each covered entity that may qualify as a hybrid entity and will be influenced by factors such as how the entity is organized and the proportion of the entity that must be included in the health care component. Where the non-covered functions of the entity are only a small portion of the entity, it will likely be more efficient to simply consider the entire entity as a covered entity. Nonetheless, the Department is proposing to permit flexibility for covered entities to choose whether or not to be treated as a covered entity entirely or as a hybrid entity.

The Department also proposes to simplify the definition of ''health care component'' in § 164.504(a) to make clear that a health care component is whatever the covered entity designates as the health care component, consistent with the provisions regarding designation in § 164.504(c)(3)(iii). The specific language regarding which components make up a health care component would be in the implementation specification that addresses designation of health care components. The Department proposes to move this specific language because it provides requirements and directions that are more appropriately placed in an implementation specification. The Department proposes that health care components may include: (1) Components of the covered entity that engage in covered functions, and (2) any component that engages in activities that would make such component a business associate of a component that performs covered functions if the two components were separate legal entities.

With respect to the components that perform covered functions, the Department also clarifies that a hybrid entity must include in its health care component(s) any component that would meet the definition of ''covered entity'' if it were a separate legal entity. ''Covered functions'' are those functions of a covered entity that make the entity a health plan, health care provider, or health care clearinghouse. However, there was some ambiguity as to whether a component of a covered entity that is a health care provider, but that does not conduct standard electronic transactions, must be included in the health care component. The proposed language would clarify that any component that would be a covered entity if it were a separate legal entity must be included in the health care component.

Under these proposed changes, a component that is a health care provider and that engages in standard electronic transactions must be included in the health care component, but a component that is a health care provider but that does not engage in standard electronic transactions may, but would not be required to, be included in the health care component of the hybrid entity. The decision would be left to the covered entity in the second case. For example, in a university setting, the single legal entity may operate hospital facilities that bill electronically and research laboratories that do not engage in any electronic billing. The modification would clarify that the university as a hybrid entity need only include the hospital facilities that bill electronically in the health care component. The modification also would make clear that the university has the option to include the components, such as the research laboratory, that function as a health care provider, but not as a covered health care provider. A covered entity that chooses to include a non-covered health care provider in their health care component would be required to ensure that the non-covered health care provider, as well as the rest of the health care component, is in compliance with the Privacy Rule.

There is also a conforming change in the proposed language in § 164.504(c)(1)(ii) to make it clear that a reference to a ''covered health care provider'' in the Privacy Rule could

include the functions of a health care provider who does not engage in electronic transactions, if the covered entity chooses to include such functions in the health care component.

With respect to the language regarding components that engage in ''business associate'' functions, the Department does not make any substantive change. The components of a hybrid that may provide services to the component that performs covered functions, such as a portion of the legal or accounting departments of the entity, may be included in the health care component so protected health information can be shared with such components of the entity without requiring business associate agreements or individual authorizations. The related language in paragraph (2)(ii) of the definition of ''health care component'' in the Privacy Rule that requires the ''business associate'' functions include the use of protected health information is not included in this proposed Rule because it is redundant.

It is important to note that a covered entity may include components that engage in ''business associate'' functions in its health care component or not. It is not a violation of the Privacy Rule to fail to include such a component in the health care component designation. However, a disclosure of protected health information from the health care component to such other component if it is not part of the health care component is the same as a disclosure outside the covered entity and is a violation unless it is permitted by the Privacy Rule. Because an entity cannot have a business associate contract with itself, such a disclosure likely would require individual authorization.

Finally, to avoid needless application of the hybrid entity provisions to a covered entity's activities as an employer, rather than as a health plan, health care provider, or health care clearinghouse, the Department proposes to modify the definition of ''protected health information'' in § 164.501. The preamble to the Privacy Rule makes clear that the Privacy Rule does not treat employment records as protected health information. To avoid any confusion or misinterpretation on this point, the Department proposes to expressly exclude employment records held by a covered entity in its role as employer from the definition of ''protected health information.'' In that way, employment records will be treated in the same manner as student medical records covered by FERPA, which the Privacy Rule excludes from the definition of ''protected health information.'' This change will limit the need for a covered entity, whose primary activities are covered functions, to designate itself as a hybrid entity simply to carve out employment records.

It is important to note that the exception from the definition of ''protected health information'' for employment records only applies to individually identifiable health information in those records that are held by a covered entity in its role as employer. The exception does not apply to individually identifiable health information held by a covered entity when carrying out its health plan or health care provider functions. Such information would be protected health information. The Department specifically is soliciting comments on whether the term ''employment records'' is clear or whether it needs to be more fully explained. It would be particularly helpful if commenters could identify certain types of records that should be included or excluded from ''employment records.''

7. Technical Corrections. The Privacy Rule contained some technical and typographical errors. Therefore, the Department proposes to make the following corrections:

a. In § 160.102(b), beginning in the second line, ''section 201(a)(5) of the Health Insurance Portability Act of 1996, (Pub. L. 104–191),'' is replaced with ''42 U.S.C. 1320a–7c(a)(5)''.

b. In § 160.203(b), in the second line, ''health information'' is replaced with ''individually identifiable health information''.

c. In § 164.102, ''implementation standards'' is corrected to read ''implementation specifications.''

d. In § 164.501, in the definition of ''protected health information'', ''Family Educational Right and Privacy Act'' is corrected to read ''Family Educational Rights and Privacy Act.''

e. In § 164.508(b)(1)(ii), in the fifth line, the word ''be'' is deleted.

f. In § 164.508(b)(3)(iii), a comma is added after the words ''psychotherapy notes''.

g. In § 164.510(b)(3), in the third line, the word ''for'' is deleted.

h. In § 164.512(b)(1)(v)(A), in the fourth line, the word ''a'' is deleted.

i. In § 164.512(b)(1)(v)(C), in the eighth line, the word ''and'' is added after the semicolon.

j. In § 164.512(f)(3), paragraphs (ii) and (iii) are redesignated as (i) and (ii), respectively.

k. In § 164.512(g)(2), in the seventh line, the word ''to'' is added after the word ''directors.''

l. In § 164.512(i)(1)(iii)(A), in the second line, the word ''is'' after the word ''sought'' is deleted.

m. In § 164.522(a)(1)(v), in the sixth line, ''§§ 164.502(a)(2)(i)'' is corrected to read ''§§ 164.502(a)(2)(ii)''.

n. In § 164.530(i)(4)(ii)(A), in the second line, ''the requirements'' is replaced with the word ''specifications''.

IV. Preliminary Regulatory Impact Analysis

Federal law (5 U.S.C. 804(2), as added by section 251 of Pub. L. 104–21), specifies that a ''major rule'' is any rule that the Office of Management and Budget finds is likely to result in:

- An annual effect on the economy of $100 million or more;
- A major increase in costs or prices for consumers, individual industries, federal, State, or local government agencies, or geographic regions; or
- Significant adverse effects in competition, employment, investment productivity, innovation, or on the ability of United States based enterprises to compete with foreign-based enterprises in domestic and export markets.

The impact of the modifications proposed in this rulemaking would be a net reduction of costs associated with the Privacy Rule of approximately $100 million. Therefore, this Rule is a major rule as defined in 5 U.S.C. 804(2).

Executive Order 12866 directs agencies to assess all costs and benefits of available regulatory alternatives and, when regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects; distributive impacts; and equity). According to Executive Order 12866, a regulatory action is ''significant'' if it meets any one of a number of specified conditions, including having an annual effect on the economy of $100 million or more, adversely affecting in a material way a sector of the economy, competition, or jobs, or if it raises novel legal or policy issues. The purpose of the regulatory impact analysis is to assist decision-makers in understanding the potential ramifications of a regulation as it is being developed. The analysis is also intended to assist the public in understanding the general economic ramifications of the regulatory changes.

The Privacy Rule included a regulatory impact analysis (RIA), which estimated the cost of the Privacy Rule at $17.6 billion over ten years. 65 FR 82462, 82758. The changes to the Privacy Rule proposed by this notice of proposed rulemaking are a result of comment by the industry and the public at large identifying a number of unintended consequences of the Privacy

Rule that could adversely affect access to, or the quality of health care delivery. These proposed changes should facilitate implementation and compliance with the Privacy Rule, and lower the costs and burdens associated with the Privacy Rule while maintaining the confidentiality of protected health information.

The proposed changes would affect five areas of the Privacy Rule that will have an economic impact: (1) Consent; (2) notice; (3) marketing; (4) research; and (5) business associates. In addition, the proposal contains a number of changes that, though important, can be categorized as clarifications of intended policy. For example, the modifications would permit certain uses and disclosures of protected health information that are incidental to an otherwise permitted use or disclosure. This change would recognize such practices as the need for physicians to talk to patients in semi-private hospital rooms or nurses to communicate with others in public areas, and avoids the costs covered entities might have incurred to reconfigure facilities as necessary to ensure absolute privacy for these common treatment-related communications. This and other modifications in this proposal (other than those described below) clarify the intent of the standards in the Privacy Rule and, as such, do not change or alter the associated costs that were estimated for the Privacy Rule. There are no new costs or savings by these changes, and therefore, there is no cost estimate made here for them.

A. Summary of Costs and Benefits in Final Regulatory Impact Statement

The Privacy Rule was estimated to produce net costs of $17.6 billion, with net present value costs of $11.8 billion (2003 dollars) over ten years (2003–2012). The Department estimates the modifications in this proposal would lower the net cost of the Privacy Rule by approximately $100 million over ten years.

Measuring both the economic costs and benefits of health information privacy was recognized as a difficult task. The paucity of data and incomplete information on current industry privacy and information system practices made cost estimation a challenge. Benefits were difficult to measure because they are, for the most part, inherently intangible. Therefore, the regulatory impact analysis in the Privacy Rule focused on the key policy areas addressed by the privacy standards, some of which would be affected by the proposed modifications in this rulemaking.

B. Proposed Modifications To Prevent Barriers to Access to or Quality of Health Care

The changes proposed in this rulemaking are intended to address the possible adverse effects of the final privacy standards on an individual's access to, or the quality of, health care. The modifications touch on five of the key policy areas addressed by the final regulatory impact analysis, including consent, research, marketing, notice, and business associates.

Consent

Under the Privacy Rule, a covered health care provider with a direct treatment relationship with an individual must obtain the individual's prior written consent for use or disclosure of protected health information for treatment, payment, or health care operations, subject to a limited number of exceptions. Other covered health care providers and health plans may obtain such a consent if they so choose. The initial cost of the consent requirement was estimated to be $42 million. Based on assumptions for growth in the number of patients, the total costs for ten years was estimated to be $103 million. *See* 65 FR 82771 (December 28, 2000).[2]

The proposed modifications would eliminate the consent requirement. The consent requirement posed many difficulties for an individual's access to health care, and was problematic for operations essential for the quality of the health care delivery system. However, any health care provider or health plan may choose to obtain an individual's consent for treatment, payment, and health care operations. The elimination of the consent requirement reduces the initial cost of the privacy standards by $42 million in the first year and by $103 million over ten years.

As explained in detail in section III.A.1. above, many comments that the Department received in March 2001 and testimony before the NCVHS revealed that the consent requirements in the Privacy Rule create unintended barriers to timely provision of care, particularly with respect to use and disclosure of health information prior to a health care provider's first face-to-face contact with the individual. These and other barriers discussed above would have entailed costs not anticipated in the economic analyses in the Privacy Rule. These comments also revealed that the consent requirements create administrative burdens, for example, with respect to tracking the status and revocation of consents, that were not foreseen and thus not included in that economic analysis. Therefore, while the estimated costs of the consent provisions were $103 million, comments have suggested that the costs were likely to be much higher. If these comments are accurate, the cost savings associated with retracting the consent provisions would, therefore, also be significantly higher than $103 million.

Notice

In eliminating the consent requirement, the Department proposes to preserve the opportunity for a covered health care provider with a direct treatment relationship with an individual to engage in a meaningful communication about the provider's privacy practices and the individual's rights by strengthening the notice requirements. Under the Privacy Rule, these health care providers are required to distribute to individuals their notice of privacy practices no later than the date of the first service delivery after the compliance date. The modifications would not change this distribution requirement, but would add a new documentation requirement. A covered health care provider with a direct treatment relationship would be required to make a good faith effort to obtain the individual's acknowledgment of receipt of the notice provided at the first service delivery. The form of the acknowledgment is not prescribed and can be as unintrusive as retaining a copy of the notice initialed by the individual. If the provider's good faith effort fails, documentation of the attempt is all that would be required. Since the modification would not require any change in the form of the notice or its distribution, the ten-year cost estimate of $391 million for these areas in the Privacy Rule's impact analysis remains the same. *See* 65 FR 82770 (December 28, 2000).

However, the additional effort by direct treatment providers in obtaining and documenting the individual's acknowledgment of receipt of the notice would add costs. This new requirement would attach only to the initial provision of notice by a direct treatment provider to an individual after the compliance date. Under the proposed modification, providers would have considerable flexibility on how to achieve this. Some providers could

[2] The total cost for consent in the regulatory impact analysis showed an initial cost of $166 million and $227 million over ten years. Included in these total numbers is the cost of tracking patient requests to restrict the disclosure of their health information. This right is not changed in these modifications. The numbers here represent the costs associated with the consent functions that are proposed to be repealed.

choose to obtain the required written acknowledgment on a separate piece of paper, while others could take different approaches, such as an initialed check-off sheet or a signature line on the notice itself with the provider keeping a copy.

In the original analysis, the Department estimated that the consent cost would be $0.05 per page based on the fact that the consent had to be a stand alone document requiring a signature. This proposed modification to the notice requirement would provide greater flexibility and, therefore, greater opportunity to reduce costs compared to the consent requirement. The Department estimates that the additional cost of the signature requirement, on average, would be $0.03 per notice. Based on data obtained from the Medical Expenditure Panel Survey (MEPS), which estimate the number of patient visits in a year, the Department estimates that in the first year there would be 816 million notices distributed, including the new additional information needed to acknowledge receipt of the notice. Over the next nine years, the Department estimates, again based on MEPS data, that there would be 5.3 billion visits to health care providers by new patients (established patients will not need to receive another copy of the notice). At $0.03 per document, the first year cost would be $24 million and the total cost over ten years would be $184 million.

Business Associates

The Privacy Rule requires a covered entity to have a written contract, or other arrangement that documents satisfactory assurances that a business associate will appropriately safeguard protected health information in order to disclose protected health information to the business associate. The regulatory impact analysis for the Privacy Rule provided cost estimates for two aspects of this requirement. In the Privacy Rule, $103 million in first-year costs was estimated for development of a standard business associate contract language. (There were additional costs associated with these requirements related to the technical implementation of new data transfer protocols, but these are not affected by the changes being proposed here.) In addition, $197 million in first-year costs and $697 million in total costs over ten years were estimated in the Privacy Rule for the review and oversight of existing business associate contracts.

The modifications do not change the standards for business associate contracts or the implementation specifications with respect to the covered entity's responsibilities for managing the contracts. However, as part of this proposal, the Department is including model business associate contract language. This model is only suggested language and is not a complete contract. The model language is designed to be adapted to the business arrangement between the covered entity and the business associate and to be incorporated into a contract drafted by the parties. The final regulatory impact analysis assumed the development of such standard language by trade and professional associations. While this has, in fact, been occurring, the Department continues to receive requests for model contract language, particularly from small health care providers. The Department expects that trade and professional associations will continue to provide assistance to their members. However, the model contract language in this proposal will simplify their efforts by providing a base from which they can develop language. The Department had estimated $103 million in initial year costs for this activity based on the assumption it would require one hour per non-hospital provider and two hours for hospitals and health plans to develop contract language and to tailor the language to the particular needs of the covered entity. The additional time for hospitals and health plans reflected the likelihood that these covered entities would have a more extensive number of business associate relationships. Because there will be less effort expended than originally estimated in the Privacy Rule, the Department estimates a reduction in contract development time by one-third because of the availability of the model language. Thus, the Department now estimates that this activity will take 40 minutes for non-hospital providers and 80 minutes for hospitals and health plans. The Department estimates that the savings from the proposed business associate contract language would be approximately $35 million in the first year.

The Department is also proposing in this rulemaking to give covered entities additional time to review their existing business associate contracts and to conform written contracts to the privacy standards. Under the proposal, a covered entity's written business associate contracts, existing at the time the modifications become effective, would be deemed to comply with the privacy standards until such time as the contracts are renewed or modified or until April 14, 2004, whichever is earlier. The effect of this proposal would be to spread first year costs over an additional year, with a corresponding postponement of the costs estimated for the out years. However, the Department has no reliable information as to the number of contracts potentially affected by the modification or how long a delay may occur. Therefore, the Department does not compute any cost savings to this modification.

Marketing

Under § 164.514(e) of the Privacy Rule, certain health-related communications are subject to special conditions on marketing communications, if they also serve to promote the use or sale of a product or service. These marketing conditions require that particular disclosures be made as part of the marketing materials sent to individuals. Absent these disclosures, protected health information can only be used or disclosed in connection with such marketing communications with the individual's authorization. The Department is aware that the Privacy Rule's § 164.514(e) conditions for health-related communications create a potential burden on covered entities to make difficult assessments regarding many of their communications. The proposed modifications to the marketing provisions would relieve the burden on covered entities by making most marketing subject to an authorization requirement and eliminating the § 164.514(e) conditions on marketing communications.

In developing the final impact analysis for the Privacy Rule, the Department was unable to estimate the cost of the marketing provisions. There was too little data and too much variation in current practice to estimate how the Privacy Rule might affect marketing. The same remains true today. However, the proposed modifications would relieve burden on the covered entities in making communications for treatment and certain health care operations relative to the requirements in the Privacy Rule. Although the Department cannot provide a quantifiable estimate, the effect of these proposed changes will be to lower costs relative to the Privacy Rule.

Research

In the final impact analysis for the Privacy Rule, the Department estimated the total cost of the provisions requiring documentation of an Institutional Review Board (IRB) or Privacy Board waiver of individual authorization for the use or disclosure of protected health information for a research purpose as $40 million for the first year and $585

million for the ten-year period. The costs were estimated based on the time that an IRB or privacy board would need to consider a request for a waiver under the criteria provided in the Privacy Rule. See 65 FR 82770–82771 (December 28, 2000).

The proposed modification would simplify and reduce the number of criteria required for an IRB or Privacy Board to approve a waiver of authorization in three ways. First, the proposal would simplify the criteria for waivers to better conform to the Common Rule's waiver criteria for informed consent to participate in the research study. Second, the proposal would simplify the accounting procedures for research by eliminating the need to account for disclosures based on individual authorization. Third, the proposal would simplify the authorization process for research to facilitate the combining of the informed consent for participation in the research itself with all authorizations required under the Privacy Rule. Therefore, the Department estimates that the net effect of these modifications would be to reduce the time necessary to assemble the necessary waivers and for an IRB or Privacy Board to consider and act on waiver requests by one quarter. The Department estimates these simplifications would reduce the expected costs first year costs by $10 million and the ten year costs by $146 million, relative to the Privacy Rule. Since this initial estimate is based on limited information available to the Department, the Department requests information to better assess this cost savings.

PRIVACY RULE MODIFICATIONS—TEN-YEAR COST ESTIMATES

Policy	Original Cost	Modification	Change due to modification
Consent	$103 million	Provision removed	−$103 million.[1]
Notice	$391 million	Good faith effort to obtain acknowledgment of receipt .	+$184 million.
Marketing	Not scored due to lack of data .	Fewer activities constitute marketing .	Reduction in cost but magnitude cannot be estimated.
Business Associates	$103 million for contract modifications .	Model language provided	−$35 million.
Research	$585 million	Waiver requirements simplified .	−$146 million.
Net Change			−$100 million.

[1] As noted above in the discussion on consent, while the estimated costs of the consent provisions were $103 million, comments have suggested that the costs were likely to be much higher. If these comments are accurate, the cost savings associated with retracting the consent provisions would, therefore, also be significantly higher than $103 million.

C. Costs to the Federal Government

The proposed changes in this Rule will result in small savings to the federal government relative to the costs that would have occurred under the Privacy Rule. Although there will be some increase in costs for the new requirements for obtaining acknowledgment for receipt of the notice, these costs are partially offset by the savings in the elimination of the consent. As discussed above, to the extent comments are accurate that the costs for the consent provisions are much higher than estimated, the cost savings associated with the retraction of these provisions would, therefore, be significantly higher. The Department does not believe the federal government engages in significant marketing as defined in the Privacy Rule. The federal government will have business associates under the Privacy Rule, and therefore, the model language proposed in this rulemaking will be of benefit to federal departments and agencies. The Department has not estimated the federal government's portion of the $35 million savings it estimated for this change. Similarly, the federal government, which conducts and sponsors a significant amount of research that is subject to IRBs, will realize some savings as a result of the research modifications proposed in this rulemaking. The Department does not have sufficient information, however, to estimate the federal government's portion of the total $146 million savings with respect to research modifications.

D. Costs to State and Local Government

The proposed changes also may affect the costs to state and local governments. However, these effects likely will be small. As with the federal government, state and local governments will have any costs of the additional notice requirement offset by the savings realized by the elimination of the consent requirement. As discussed above, to the extent comments are accurate that the costs for the consent provisions are much higher than estimated, the cost savings associated with the retraction of these provisions would, therefore, be significantly higher. State and local governments could realize savings from the model language for business associates and the changes in research, but the savings are likely to be small. The Department does not have sufficient information to estimate the state and local government's share of the net savings from the proposed changes.

E. Benefits

The benefits of these modifications would be lower costs, and enhanced implementation and compliance with the Privacy Rule without compromising the protection of individually identifiable health information or access to quality health care.

F. Alternatives

In July 2001, the Department clarified the Privacy Rule in guidance, where feasible, to resolve some of the issues raised by commenters. Issues that could not adequately be addressed through guidance because of the need for a regulatory change are addressed in this proposed Rule. The Department examined a number of alternatives to these proposed provisions. One alternative was to not make any changes to the Privacy Rule, but this option was rejected for the reasons explained throughout the preamble. The Department also considered various alternatives to specific provisions in the development of this proposed Rule. These alternatives are generally discussed above, where appropriate.

V. Preliminary Regulatory Flexibility Analysis

The Department also examined the impact of this proposed Rule as required

by the Small Business Regulatory Enforcement and Fairness Act (SBREFA) (5 U.S.C. 601, *et seq.*). SBREFA requires agencies to determine whether a rule will have a significant economic impact on a substantial number of small entities.

The law does not define the thresholds to use in implementing the law and the Small Business Administration discourages establishing quantitative criteria. However, the Department has long used two criteria—the number of entities affected and the impact on revenue and costs—for assessing whether a regulatory flexibility analysis is necessary. Department guidelines state that an impact of three to five percent should be considered a significant economic impact. Based on these criteria, the Department has determined that a regulatory flexibility analysis is not required.

As described in the Regulatory Flexibility Analysis for the Privacy Rule, most covered entities are small businesses—approximately 465,000. *See* Table A, 65 FR 82780 (December 28, 2000). Lessening the burden for small entities, consistent with the intent of protecting privacy, was an important consideration in developing these modifications. However, as discussed in the Preliminary Regulatory Impact Analysis, above, the net affect of the proposed changes is an overall savings of approximately $100 million over ten years. Even if all of this savings were to accrue to small entities (an over estimation), the impact per small entity would be de minimis.

VI. Collection of Information Requirements

Under the Paperwork Reduction Act (PRA) of 1995, the Department is required to provide 60-day notice in the **Federal Register** and solicit public comment before a collection of information requirement is submitted to the Office of Management and Budget (OMB) for review and approval. In order to fairly evaluate whether an information collection should be approved by OMB, section 3506(c)(2)(A) of the PRA requires that the Department solicit comment on the following issues:

- The need for the information collection and its usefulness in carrying out the proper functions of the agency.
- The accuracy of the estimate of the information collection burden.
- The quality, utility, and clarity of the information to be collected.
- Recommendations to minimize the information collection burden on the affected public, including automated collection techniques.

In accordance with these requirements, the Department is soliciting public comments on the model business associate contract language displayed in the Appendix to this proposed Rule. The Department provides these model business associate contract provisions in response to numerous requests for guidance. These provisions are designed to help covered entities more easily comply with the business associate contract requirements of the Privacy Rule. However, use of these model provisions is not required for compliance with the Privacy Rule. Nor is the model language a complete contract. Rather, the model language is designed to be adapted to the business arrangement between the covered entity and the business associate and to be incorporated into a contract drafted by the parties.

Section 164.506—Consent for Treatment, Payment, and Health Care Operations

Under the Privacy Rule, a covered health care provider that has a direct treatment relationship with individuals must, except in certain circumstances, obtain an individual's consent to use or disclose protected health information to carry out treatment, payment, and health care operations. The modifications would eliminate this requirement. While the consent requirement is subject to the PRA, the Department believes that the burden associated with the requirement is exempt from the PRA as stipulated under 5 CFR 1320.3(b)(2). Therefore, the modification does not affect the paperwork burden associated with the Privacy Rule.

Section 164.520—Notice of Privacy Practices for Protected Health Information

The modifications would impose a good faith effort on direct treatment providers to obtain an individual's acknowledgment of receipt of the notice of privacy practices for protected health information and to document such acknowledgment or, in the absence of such acknowledgment, the entity's good faith efforts to obtain it. In addition, a covered entity would have to retain the acknowledgment or documentation of the good faith effort as required by § 164.530(j). The Department is continuing to work on estimating the burden imposed by the Privacy Rule. The estimate for the acknowledgment of receipt of the notice will be reflected in the paperwork reduction package to be submitted to OMB as required by the PRA.

The Department has submitted a copy of this proposed Rule to OMB for its review of the information collection requirements described above. These requirements are not effective until they have been approved by OMB.

If you comment on any of these information collection and record keeping requirements, please mail copies directly to the following:

Center for Medicaid and Medicare Services, Information Technology Investment Management Group, Division of CMS Enterprise Standards, Room C2–26–17, 7500 Security Boulevard, Baltimore, MD 21244–1850. ATTN: John Burke, HIPAA Privacy;

and

Office of Information and Regulatory Affairs, Office of Management and Budget, Room 10235, New Executive Office Building, Washington, DC 20503, ATTN: Allison Herron Eydt, CMS Desk Officer.

VII. Unfunded Mandates

Section 202 of the Unfunded Mandates Reform Act of 1995 also requires that agencies assess anticipated costs and benefits before issuing any rule that may result in an expenditure by State, local, or tribal governments, in the aggregate, or by the private sector, of $110 million in a single year. A final cost-benefit analysis was published in the Privacy Rule of December 28, 2000 (65 FR 82462, 82794). In developing the final Privacy Rule, the Department adopted the least burdensome alternatives, consistent with achieving the Rule's goals. The Department does not believe that the modifications in the proposed Rule would qualify as an unfunded mandate under the statute.

VIII. Environmental Impact

The Department has determined under 21 CFR 25.30(k) that this action is of a type that does not individually or cumulatively have a significant effect on the human environment. Therefore, neither an environmental assessment nor an environmental impact statement is required.

IX. Executive Order 13132: Federalism

Executive Order 13132 establishes certain requirements that an agency must meet when it promulgates a proposed rule (and subsequent Privacy Rule) that imposes substantial direct requirement costs on State and local governments, preempts State law, or otherwise has Federalism implications. The federalism implications of the Privacy Rule were assessed as required by Executive Order 13132 and published in the Privacy Rule of

December 28, 2000 (65 FR 82462, 82797). The proposed change with the most direct effect on federalism principles concerns the clarifications regarding the rights of parents and minors under State law. The modifications would make clear the intent of the Department to defer to State law with respect to such rights. Therefore, the Department believes that the modifications in this proposed Rule would not significantly affect the rights, roles and responsibilities of States.

Appendix to the Preamble—Model Business Associate Contract Provisions

Introduction

The Department of Health and Human Services provides these model business associate contract provisions in response to numerous requests for guidance. This is only model language. These provisions are designed to help covered entities more easily comply with the business associate contract requirements of the Privacy Rule. However, use of these model provisions is not required for compliance with the Privacy Rule. The language may be amended to more accurately reflect business arrangements between the covered entity and the business associate.

These or similar provisions may be incorporated into an agreement for the provision of services between the entities or they may be incorporated into a separate business associate agreement. These provisions only address concepts and requirements set forth in the Privacy Rule and alone are not sufficient to result in a binding contract under State law and do not include many formalities and substantive provisions that are required or typically included in a valid contract. Reliance on this model is not sufficient for compliance with state law and does not replace consultation with a lawyer or negotiations between the parties to the contract.

Furthermore, a covered entity may want to include other provisions that are related to the Privacy Rule but that are not required by the Privacy Rule. For example, a covered entity may want to add provisions in a business associate contract in order for the covered entity to be able to rely on the business associate to help the covered entity meet its obligations under the Privacy Rule. In addition, there may be permissible uses or disclosures by a business associate that are not specifically addressed in these model provisions. For example, the Privacy Rule does not preclude a business associate from disclosing protected health information to report unlawful conduct in accordance with § 164.502(j). However, there is not a specific model provision related to this permissive disclosure. These and other types of issues will need to be worked out between the parties.

Model Business Associate Contract Provisions [1]

Definitions (alternative approaches)

Catch-all definition:

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in 45 CFR 160.103 and 164.501.

Examples of specific definitions:

(a) *Business Associate.* ''Business Associate'' shall mean [Insert Name of Business Associate].

(b) *Covered Entity.* ''Covered Entity'' shall mean [Insert Name of Covered Entity].

(c) *Individual.* ''Individual'' shall have the same meaning as the term ''individual'' in 45 CFR 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

(d) *Privacy Rule.* ''Privacy Rule'' shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.

(e) *Protected Health Information.* ''Protected Health Information'' shall have the same meaning as the term ''protected health information'' in 45 CFR 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

(f) *Required By Law.* ''Required By Law'' shall have the same meaning as the term ''required by law'' in 45 CFR 164.501.

(g) *Secretary.* ''Secretary'' shall mean the Secretary of the Department of Health and Human Services or his designee.

Obligations and Activities of Business Associate

(a) Business Associate agrees to not use or further disclose Protected Health Information other than as permitted or required by the Agreement or as Required By Law.

(b) Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.

(c) Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement. [This provision may be included if it is appropriate for the Covered Entity to pass on its duty to mitigate damages by a Business Associate.]

(d) Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement.

(e) Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

(f) Business Associate agrees to provide access, at the request of Covered Entity, and in the time and manner designated by Covered Entity, to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR 164.524. [Not necessary if business associate does not have protected health information in a designated record set.]

(g) Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR 164.526 at the request of Covered Entity or an Individual, and in the time and manner designated by Covered Entity. [Not necessary if business associate does not have protected health information in a designated record set.]

(h) Business Associate agrees to make internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to the Covered Entity, or at the request of the Covered Entity to the Secretary, in a time and manner designated by the Covered Entity or the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

(i) Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

(j) Business Associate agrees to provide to Covered Entity or an Individual, in time and manner designated by Covered Entity, information collected in accordance with Section [Insert Section Number in Contract Where Provision (i) Appears] of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

Permitted Uses and Disclosures by Business Associate

General Use and Disclosure Provisions (alternative approaches)

Specify purposes:

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information on behalf of, or to provide services to, Covered Entity for the following purposes, if such use or disclosure of Protected Health Information would not violate the Privacy Rule if done by Covered Entity: [List Purposes].

Refer to underlying services agreement:

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in [Insert Name of Services Agreement], provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity.

[1] Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these model provisions and are not intended to be included in the contractual provisions.

Specific Use and Disclosure Provisions [only necessary if parties wish to allow Business Associate to engage in such activities]

(a) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

(b) Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(c) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 42 CFR 164.504(e)(2)(i)(B).

Obligations of Covered Entity

Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions [provisions dependent on business arrangement]

(a) Covered Entity shall provide Business Associate with the notice of privacy practices that Covered Entity produces in accordance with 45 CFR 164.520, as well as any changes to such notice.

(b) Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, if such changes affect Business Associate's permitted or required uses and disclosures.

(c) Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR 164.522.

Permissible Requests by Covered Entity

Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity. [Include an exception if the Business Associate will use or disclose protected health information for, and the contract includes provisions for, data aggregation or management and administrative activities of Business Associate].

Term and Termination

(a) *Term.* The Term of this Agreement shall be effective as of [Insert Effective Date], and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section.

(b) *Termination for Cause.* Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement [and the ____ Agreement/sections ____ of the ____ Agreement] if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity, or immediately terminate this Agreement [and the ____ Agreement/sections ____ of the ____ Agreement] if Business Associate has breached a material term of this Agreement and cure is not possible. [Bracketed language in this provision may be necessary if there is an underlying services agreement. Also, opportunity to cure is permitted, but not required by the Privacy Rule.]

(c) *Effect of Termination.*

(1) Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

(2) In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

Miscellaneous

(a) *Regulatory References.* A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended, and for which compliance is required.

(b) *Amendment.* The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act, Public Law 104–191.

(c) *Survival.* The respective rights and obligations of Business Associate under Section [Insert Section Number Related to ''Effect of Termination''] of this Agreement shall survive the termination of this Agreement.

(d) *Interpretation.* Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with the Privacy Rule.

List of Subjects

45 CFR Part 160

Electronic transactions, Employer benefit plan, Health, Health care, Health facilities, Health insurance, Health records, Medicaid, Medical research, Medicare, Privacy, Reporting and record keeping requirements.

45 CFR Part 164

Electronic transactions, Employer benefit plan, Health, Health care, Health facilities, Health insurance, Health records, Medicaid, Medical research, Medicare, Privacy, Reporting and record keeping requirements.

Dated: March 12, 2002.

Tommy G. Thompson,

Secretary.

For the reasons set forth in the preamble, the Department proposes to amend 45 CFR Subtitle A, Subchapter C, as follows:

PART 160—GENERAL ADMINISTRATIVE REQUIREMENTS

1. The authority citation for part 160 continues to read as follows:

Authority: Sec. 1171 through 1179 of the Social Security Act, (42 U.S.C. 1320d–1329d–8) as added by sec. 262 of Pub. L. 104–191, 110 Stat. 2021–2031 and sec. 264 of Pub. L. 104–191 (42 U.S.C. 1320d–2(note)).

§ 160.102 [Amended]

2. Amend § 160.102(b), by removing the phrase ''section 201(a)(5) of the Health Insurance Portability Act of 1996, (Pub. L. 104–191)'' and adding in its place the phrase ''the Social Security Act, 42 U.S.C. 1320a–7c(a)(5)''.

3. In § 160.103 add the definition of ''individually identifiable health information'' in alphabetical order to read as follows:

§ 160.103 Definitions.

* * * * *

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

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

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

(i) That identifies the individual; or

(ii) With respect to which there is a reasonable basis to believe the

information can be used to identify the individual.

* * * * *

4. In § 160.202 revise paragraphs (2) and (4) of the definition of ''more stringent'' to read as follows:

§ 160.202 Definitions.

* * * * *

More stringent means * * *

(2) With respect to the rights of an individual, who is the subject of the individually identifiable health information, regarding access to or amendment of individually identifiable health information, permits greater rights of access or amendment, as applicable.

* * * * *

(4) With respect to the form, substance, or the need for express legal permission from an individual, who is the subject of the individually identifiable health information, for use or disclosure of individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the express legal permission, as applicable.

* * * * *

§ 160.203 [Amended]

5. Amend § 160.203(b) by adding the words ''individually identifiable'' before the word ''health''.

PART 164—SECURITY AND PRIVACY

Subpart E—Privacy of Individually Identifiable Health Information

1. The authority citation for part 164 continues to read as follows:

Authority: 42 U.S.C. 1320d–2 and 1320d–4, sec. 264 of Pub. L. 104–191, 110 Stat. 2033–2034 (42 U.S.C. 1320d–2(note)).

§ 164.102 [Amended]

2. Amend § 164.102 by removing the words ''implementation standards'' and adding in its place the words ''implementation specifications.''

§ 164.500 [Amended]

3. In § 164.500, remove ''consent,'' from paragraph (b)(1)(v).

§ 164.501 [Amended]

4. Amend § 164.501 as follows:

a. In the definition of ''health care operations'' remove from the introductory text of the definition '', and any of the following activities of an organized health care arrangement in which the covered entity participates'' and revise paragraphs (6)(iv) and (v).

b. Remove the definition of ''individually identifiable health information''.

c. Revise the definition of ''marketing''.

d. In paragraph (1)(ii) of the definition of ''payment,'' remove the word ''covered''.

e. Revise paragraph (2) of the definition of ''protected health information''.

The revisions read as follows:

§ 164.501 Definitions.

* * * * *

Health care operations means * * *

(6) * * *

(iv) The sale, transfer, merger, or consolidation of all or part of a covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and

(v) Consistent with the applicable requirements of § 164.514, creating de-identified health information and fundraising for the benefit of the covered entity.

* * * * *

Marketing means to make a communication about a product or service to encourage recipients of the communication to purchase or use the product or service. *Marketing* excludes a communication made to an individual:

(1) To describe the entities participating in a health care provider network or health plan network, or to describe if, and the extent to which, a product or services (or payment for such product or service) is provided by a covered entity or included in a plan of benefits;

(2) For treatment of that individual; or

(3) For case management or care coordination for that individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to that individual.

* * * * *

Protected health information means * * *

(2) *Protected health information* excludes individually identifiable health information in:

(i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;

(ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and

(iii) Employment records held by a covered entity in its role as employer.

* * * * *

5. Amend § 164.502 as follows:

a. Revise paragraphs (a)(1)(ii), (iii), and (vi).

b. Revise paragraph (b)(2)(ii).

c. Redesignate paragraphs (b)(2)(iii) through (v) as paragraphs (b)(2)(iv) through (vi).

d. Add a new paragraph (b)(2)(iii).

e. Redesignate paragraphs (g)(3)(i) through (iii) as (g)(3)(i)(A) through (C) and redesignate paragraph (g)(3) as (g)(3)(i).

f. Add new paragraphs (g)(3)(ii) and (iii).

The revisions and additions read as follows:

§ 164.502 Uses and disclosures of protected health information: general rules.

(a) *Standard.* * * *

(1) *Permitted uses and disclosures.* * * *

(ii) For treatment, payment, or health care operations, as permitted by and in compliance with § 164.506;

(iii) As incident to a use or disclosure otherwise permitted or required by this subpart, provided that the covered entity has complied with the applicable requirements of § 164.502(b), § 164.514(d), and § 164.530(c) with respect to such otherwise permitted or required uses or disclosures;

* * * * *

(vi) As permitted by and in compliance with this section, § 164.512, or § 164.514(f) and (g).

* * * * *

(b) *Standard: Minimum necessary.* * * *

(2) *Minimum necessary does not apply.* * * *

(ii) Uses or disclosures made to the individual, as permitted under paragraph (a)(1)(i) of this section or as required by paragraph (a)(2)(i) of this section;

(iii) Uses or disclosures made pursuant to an authorization under § 164.508;

* * * * *

(g)(1) *Standard: Personal representatives.* * * *

(3) *Implementation specification: unemancipated minors.*

(i) * * *

(ii) Notwithstanding the provisions of paragraph (g)(3)(i) of this section:

(A) A covered entity may disclose protected health information about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis* if an applicable provision of State or other law, including applicable case law, permits or requires such disclosure; and

(B) A covered entity may not disclose protected health information about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis* if an applicable provision of State or other law, including applicable case law, prohibits such disclosure.

(iii) Notwithstanding the provisions of paragraph (g)(3)(i) of this section, a covered entity must, consistent with State or other applicable law, provide a right of access, as set forth in § 164.524 to either:

(A) A parent, guardian, or other person acting *in loco parentis,* as the personal representative of the unemancipated minor;

(B) The unemancipated minor; or

(C) Both.

* * * * *

6. Amend § 164.504 as follows:

a. In paragraph (a), revise the definitions of ''health care component'' and ''hybrid entity''.

b. Revise paragraph (c)(1)(ii).

c. Revise paragraph (c)(3)(iii).

d. Revise paragraph (f)(1)(i).

e. Add paragraph (f)(1)(iii).

The revisions and addition read as follows:

§ 164.504 Uses and disclosures: Organizational requirements.

(a) *Definitions.* * * *

Health care component means a component or combination of components of a hybrid entity designated by the hybrid entity in accordance with paragraph (c)(3)(iii) of this section.

Hybrid entity means a single legal entity:

(1) That is a covered entity;

(2) Whose business activities include both covered and non-covered functions; and

(3) That designates health care components in accordance with paragraph (c)(3)(iii) of this section.

* * * * *

(c)(1) *Implementation specification: Application of other provisions.* * * *

(ii) A reference in such provision to a ''health plan,'' ''covered health care provider,'' or ''health care clearinghouse'' refers to a health care component of the covered entity if such health care component performs the functions of a health plan, health care provider, or health care clearinghouse, as applicable; and

* * * * *

(3) *Implementation specifications: Responsibilities of the covered entity.* * * *

(iii) The covered entity is responsible for designating the components that are part of one or more health care components of the covered entity and documenting the designation as required by § 164.530(j), provided that if the covered entity designates a health care component or components, it must include any component that would meet the definition of covered entity if it were a separate legal entity. Health care component(s) may include a component that performs:

(A) covered functions; and

(B) activities that would make such component a business associate of a component that performs covered functions if the two components were separate legal entities.

* * * * *

(f)(1) *Standard: Requirements for group health plans.* (i) Except as provided under paragraph (f)(1)(ii) or (iii) of this section or as otherwise authorized under § 164.508, a group health plan, in order to disclose protected health information to the plan sponsor or to provide for or permit the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO with respect to the group health plan, must ensure that the plan documents restrict uses and disclosures of such information by the plan sponsor consistent with the requirements of this subpart.

* * * * *

(iii) The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose to the plan sponsor information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan to the plan sponsor.

* * * * *

7. Revise § 164.506 to read as follows:

§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations.

(a) *Standard: Permitted uses and disclosures.* Except with respect to uses or disclosures that require an authorization under § 164.508(a)(2) and (3), a covered entity may use or disclose protected health information for treatment, payment, or health care operations as set forth in paragraph (c) of this section, provided that such use or disclosure is consistent with other applicable requirements of this subpart.

(b) *Standard: Consent permitted.* (1) A covered entity may obtain consent of the individual to use or disclose protected health information to carry out treatment, payment, or health care operations.

(2) Consent of an individual under this paragraph shall not be effective to permit a use or disclosure of protected health information that is not otherwise permitted or required by this subpart.

(c) *Implementation specifications: Treatment, payment, or health care operations.*

(1) A covered entity may use or disclose protected health information for its own treatment, payment, or health care operations.

(2) A covered entity may disclose protected health information for treatment activities of another health care provider.

(3) A covered entity may disclose protected health information to another covered entity or health care provider for the payment activities of the entity that receives the information.

(4) A covered entity may disclose protected health information to another covered entity for health care operations activities of the entity that receives the information, if both entities have a relationship with the individual who is the subject of the protected health information being requested, and the disclosure is:

(i) For a purpose listed in paragraph (1) or (2) of the definition of health care operations; or

(ii) For the purpose of health care fraud and abuse detection or compliance.

(5) A covered entity that participates in an organized health care arrangement may disclose protected health information about an individual to another covered entity that participates in the organized health care arrangement for any health care operations activities of the organized health care arrangement.

8. Amend § 164.508 as follows:

a. Remove ''consistent with consent requirements in § 164.506'' in paragraph (a)(2)(i).

b. Add ''the'' before ''originator'' in paragraph (a)(2)(i)(A).

c. Remove the word ''in'' after the term ''covered entity'' and add in its place the words ''for its own'' in paragraph (a)(2)(i)(B).

d. Add the words ''itself in'' after the word ''defend'' in paragraph (a)(2)(i)(C).

e. Add paragraph (a)(3).

f. Revise paragraphs (b)(1)(i).

g. Remove the word ''be'' in paragraph (b)(1)(ii).

h. Remove '', (d), (e), or (f)'' from paragraph (b)(2)(ii).

i. Remove paragraph (b)(2)(iv).

j. Redesignate paragraphs (b)(2)(v) and (vi) as paragraphs (b)(2)(iv) and (v).

k. Add ''or (4)'' after ''(b)(3)'' in redesignated paragraph (b)(2)(iv).

l. Revise paragraphs (b)(3)(i).

m. Add a comma after the term ''psychotherapy notes'' in paragraph (b)(3)(iii).

n. Remove ''under paragraph (f) of'' and add in its place ''for the use or disclosure of protected health information for such research under'' in paragraph (b)(4)(i).

o. Add the word ''and'' at the end of paragraph (b)(4)(ii)(B).

p. Remove paragraph (b)(4)(iii).

q. Redesignate paragraph (b)(4)(iv) as paragraph (b)(4)(iii).

r. Add ''or the policy itself'' after the word ''policy'' in paragraph (b)(5)(ii).

s. Remove paragraphs (d), (e), and (f).

t. Revise paragraph (c).

The revisions and addition read as follows:

§ 164.508 Uses and disclosures for which an authorization is required.

(a) *Standard: Authorizations for uses and disclosures.* * * *

(3) *Authorization required: Marketing.* (i) Notwithstanding any other provision of this subpart other than § 164.532, a covered entity must obtain an authorization for any use or disclosure of protected health information for marketing, except if the communication is in the form of:

(A) A face-to-face communication made by a covered entity to an individual; or

(B) A promotional gift of nominal value provided by the covered entity.

(ii) If the marketing is expected to result in direct or indirect remuneration to the covered entity from a third party, the authorization must state that such remuneration is expected.

* * * * *

(b) *Implementation specifications:* General requirements. * * *

(1) *Valid authorizations.*

(i) A valid authorization is a document that meets the requirements in paragraphs (c)(1) and (2) of this section.

* * * * *

(3) *Compound authorizations.* * * *

(i) An authorization for the use or disclosure of protected health information for a specific research study may be combined with any other type of written permission for the same research study, including another authorization for the use or disclosure of protected health information for such research or a consent to participate in such research;

* * * * *

(c) *Implementation specifications: Core elements and requirements.* (1) *Core elements.* A valid authorization under this section must contain at least the following elements:

(i) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.

(ii) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.

(iii) The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure.

(iv) A description of each purpose of the requested use or disclosure. The statement ''at the request of the individual'' is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.

(v) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The following statements meet the requirements for an expiration date or an expiration event if the appropriate conditions apply:

(A) The statement ''end of the research study'' or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research.

(B) The statement ''none'' or similar language is sufficient if the authorization is for the covered entity to use or disclose protected health information for the creation and maintenance of a research database or research repository.

(vi) Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.

(2) *Required statements.* In addition to the core elements, the authorization must contain statements adequate to place the individual on notice of all of the following:

(i) The individual's right to revoke the authorization in writing, and either:

(A) The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or

(B) To the extent that the information in paragraph (c)(2)(i)(A) of this section is included in the notice required by § 164.520, a reference to the covered entity's notice.

(ii) The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either:

(A) The covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations in paragraph (b)(4) of this section applies; or

(B) The consequences to the individual of a refusal to sign the authorization when, in accordance with paragraph (b)(4) of this section, the covered entity can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization.

(iii) The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected by this rule.

(3) *Plain language requirement.* The authorization must be written in plain language.

(4) *Copy to the individual.* If a covered entity seeks an authorization from an individual for a use or disclosure of protected health information, the covered entity must provide the individual with a copy of the signed authorization.

9. Amend § 164.510 as follows:

a. Revise the first sentence of the introductory text.

b. Remove the word ''for'' from paragraph (b)(3).

The revision reads as follows:

§ 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.

A covered entity may use or disclose protected health information, provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the use or disclosure, in accordance with the applicable requirements of this section. * * *

* * * * *

10. Amend § 164.512 as follows:

a. Revise the section heading and the first sentence of the introductory text.

b. Revise paragraph (b)(1)(iii).

c. In paragraph (b)(1)(v)(A) remove the word ''a'' before the word ''health.''

d. Add the word ''and'' after the semicolon at the end of paragraph (b)(1)(v)(C).

e. Redesignate paragraphs (f)(3)(ii) and (iii) as (f)(3)(i) and (ii).

f. In the second sentence of paragraph (g)(2) add the word ''to'' after the word ''directors.''

g. In paragraph (i)(1)(iii)(A) remove the word ''is'' after the word ''disclosure.''

h. Revise paragraph (i)(2)(ii).

The revisions read as follows:

§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.

A covered entity may use or disclose protected health information without the written authorization of the individual, as described in § 164.508, or the opportunity for the individual to agree or object as described in § 164.510, in the situations covered by this section,

subject to the applicable requirements of this section. * * *

* * * * *

(b) *Standard: uses and disclosures for public health activities.*

(1) *Permitted disclosures.* * * *

(iii) A person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include:

(A) To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations;

(B) To track FDA-regulated products;

(C) To enable product recalls, repairs, or replacement, or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of lookback); or

(D) To conduct post marketing surveillance;

* * * * *

(i) *Standard: Uses and disclosures for research purposes.* * * *

(2) *Documentation of waiver approval.* * * *

(ii) *Waiver criteria.* A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:

(A) The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements;

(*1*) An adequate plan to protect the identifiers from improper use and disclosure;

(*2*) An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and

(*3*) Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted by this subpart;

(B) The research could not practicably be conducted without the waiver or alteration; and

(C) The research could not practicably be conducted without access to and use of the protected health information.

* * * * *

11. Amend § 164.514 as follows:

a. Revise paragraph (b)(2)(i)(R).

b. Revise paragraph (d)(1).

c. Revise paragraph (d)(4)(iii).

d. Remove and reserve paragraph (e).

The revisions read as follows:

§ 164.514 Other requirements relating to uses and disclosures of protected health information.

* * * * *

(b) *Implementation specifications: Requirements for de-identification of protected health information.* * * *

(2)(i) * * *

(R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; and

* * * * *

(d)(1) *Standard: minimum necessary requirements.* In order to comply with § 164.502(b) and this section, a covered entity must meet the requirements of paragraphs (d)(2) through (d)(5) of this section with respect to a request for or the use and disclosure of protected health information.

* * * * *

(4) *Implementation specifications: Minimum necessary requests for protected health information.* * * *

(iii) For all other requests, a covered entity must:

(A) Develop criteria designed to limit the request for protected health information to the information reasonably necessary to accomplish the purpose for which the request is made; and

(B) Review requests for disclosure on an individual basis in accordance with such criteria.

* * * * *

(e) [Removed and Reserved]

* * * * *

12. Amend § 164.520 as follows:

a. Remove the word ''consent or'' from paragraph (b)(1)(ii)(B).

b. Revise paragraph (c)(2)(i).

c. Redesignate paragraphs (c)(2)(ii) and (iii) as (c)(2)(iii) and (iv).

d. Add new paragraph (c)(2)(ii).

e. Amend redesignated paragraph (c)(2)(iv) by removing ''(c)(2)(ii)'' and adding in its place ''(c)(2)(iii)'.

f. Revise paragraph (c)(3)(iii) by adding a sentence at the end.

g. Revise paragraph (e).

The revisions and addition read as follows:

§ 164.520 Notice of privacy practices for protected health information.

* * * * *

(c) *Implementation specifications: provision of notice.* * * *

(2) *Specific requirements for certain covered health care providers.* * * *

(i) Provide the notice:

(A) No later than the date of the first service delivery, including service delivered electronically, to such individual after the compliance date for the covered health care provider; or

(B) In an emergency treatment situation, as soon as reasonably practicable after the emergency treatment situation.

(ii) Except in an emergency treatment situation, make a good faith effort to obtain a written acknowledgment of receipt of the notice provided in accordance with paragraph (c)(2)(i) of this section, and if not obtained, document its good faith efforts to obtain such acknowledgment and the reason why the acknowledgment was not obtained;

* * * * *

(3) *Specific requirements for electronic notice.* * * *

(iii) * * * The requirements in paragraph (c)(2)(ii) of this section apply to electronic notice.

* * * * *

(e) *Implementation specifications: Documentation.* A covered entity must document compliance with the notice requirements, as required by § 164.530(j), by retaining copies of the notices issued by the covered entity and, if applicable, any written acknowledgments of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgment, in accordance with paragraph (c)(2)(ii) of this section.

§ 164.522 [Amended]

13. Amend § 164.522 by removing the reference to ''164.502(a)(2)(i)'' in paragraph (a)(1)(v), and adding in its place ''164.502(a)(2)(ii)''.

14. Amend § 164.528 as follows:

a. In paragraph (a)(1)(i), remove ''§ 164.502'' and add in its place ''§ 164.506''.

b. Redesignate paragraphs (a)(1)(iii) through (vi) as (a)(1)(iv) through (vii).

c. Add paragraph (a)(1)(iii).

d. Revise paragraph (b)(2)(iv) in its entirety.

e. Remove ''or pursuant to a single authorization under § 164.508,'' from paragraph (b)(3).

The addition and revision read as follows:

§ 164.528 Accounting of disclosures of protected health information.

(a) *Standard: Right to an accounting of disclosures of protected health information.*

(1) * * *

(iii) Pursuant to an authorization as provided in § 164.508.

* * * * *

(b) Implementation specifications: Content of the accounting. * * *

(2) * * *

(iv) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of such statement, a copy of a written request for a disclosure under §§ 164.502(a)(2)(ii) or 164.512, if any.

* * * * *

15. Amend § 164.530 as follows:

a. Redesignate paragraph (c)(2) as (c)(2)(i).

b. Add paragraph (c)(2)(ii).

c. Remove the words ''the requirements'' from paragraph (i)(4)(ii)(A) and add in their place the word ''specifications.''

The addition reads as follows:

§ 164.530 Administrative requirements.

* * * * *

(c) *Standard: Safeguards.* * * *

(2) *Implementation specifications: Safeguards.* (i) * * *

(ii) A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

* * * * *

16. Revise § 164.532 to read as follows:

§ 164.532 Transition Provisions.

(a) *Standard: Effect of prior authorizations.* Notwithstanding §§ 164.508 and 164.512(i), a covered entity may use or disclose protected health information, consistent with paragraphs (b) and (c) of this section, pursuant to an authorization or other express legal permission obtained from an individual permitting the use or disclosure of protected health information, informed consent of the individual to participate in research, or a waiver of informed consent by an IRB.

(b) *Implementation specification: Effect of prior authorization for purposes other than research.* Notwithstanding any provisions in § 164.508, a covered entity may use or disclose protected health information that it created or received prior to the applicable compliance date of this subpart pursuant to an authorization or other express legal permission obtained from an individual prior to the applicable compliance date of this subpart, provided that the authorization or other express legal permission specifically permits such use or disclosure and there is no agreed-to restriction in accordance with § 164.522(a).

(c) *Implementation specification: Effect of prior permission for research.* Notwithstanding any provisions in §§ 164.508 and 164.512(i), a covered entity may use or disclose, for a specific research study, protected health information that it created or received either before or after the applicable compliance date of this subpart, provided that there is no agreed-to restriction in accordance with § 164.522(a) and that the covered entity has obtained, prior to the applicable compliance date, either:

(1) The authorization or other express legal permission from an individual to use or disclose protected health information for the research study;

(2) The informed consent of the individual to participate in the research study; or

(3) A waiver, by an IRB, of informed consent for the research study, in accordance with 7 CFR 1c.116(d), 10 CFR 745.116(d), 14 CFR 1230.116(d), 15 CFR 27.116(d), 16 CFR 1028.116(d), 21 CFR 50.24, 22 CFR 225.116(d), 24 CFR 60.116(d), 28 CFR 46.116(d), 32 CFR 219.116(d), 34 CFR 97.116(d), 38 CFR 16.116(d), 40 CFR 26.116(d), 45 CFR 46.116(d), 45 CFR 690.116(d), or 49 CFR 11.116(d), provided that a covered entity must obtain authorization in accordance with § 164.508 if, after the compliance date, informed consent is sought from an individual participating in the research study.

(d) *Standard: Effect of prior contracts or other arrangements with business associates.* Notwithstanding any other provisions of this subpart, a covered entity, other than a small health plan, may disclose protected health information to a business associate and may allow a business associate to create, receive, or use protected health information on its behalf pursuant to a written contract or other written arrangement with such business associate that does not comply with §§ 164.502(e) and 164.504(e) consistent with the requirements, and only for such time, set forth in paragraph (e) of this section.

(e) *Implementation specification: Deemed compliance.*—(1) *Qualification.* Notwithstanding other sections of this subpart, a covered entity, other than a small health plan, is deemed to be in compliance with the documentation and contract requirements of §§ 164.502(e) and 164.504(e), with respect to a particular business associate relationship, for the time period set forth in paragraph (e)(2) of this section, if:

(i) Prior to the effective date of this provision, such covered entity has entered into and is operating pursuant to a written contract or other written arrangement with a business associate for such business associate to perform functions or activities or provide services that make the entity a business associate; and

(ii) The contract or other arrangement is not renewed or modified from the effective date of this provision and until the compliance date set forth in § 164.534.

(2) *Limited deemed compliance period.* A prior contract or other arrangement that meets the qualification requirements in paragraph (e) of this section, shall be deemed compliant until the earlier of:

(i) The date such contract or other arrangement is renewed or modified on or after the compliance date set forth in § 164.534; or

(ii) April 14, 2004.

(3) *Covered entity responsibilities.* Nothing in this section shall alter the requirements of a covered entity to comply with part 160, subpart C of this subchapter and §§ 164.524, 164.526, and 164.528 with respect to protected health information held by a business associate.

[FR Doc. 02–7144 Filed 3–21–02; 12:00 pm]

BILLING CODE 4153–01–P