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: Final rule.

SUMMARY: The Department of Health and Human Services (''HHS'' or ''Department'') modifies certain standards in the Rule entitled ''Standards for Privacy of Individually Identifiable Health Information'' (''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 these modifications is to maintain strong protections for the privacy of individually identifiable health information while clarifying certain of the Privacy Rule's provisions, addressing the unintended negative effects of the Privacy Rule on health care quality or access to health care, and relieving unintended administrative burdens created by the Privacy Rule.

DATES: This final rule is effective on October 15, 2002.

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

SUPPLEMENTARY INFORMATION:

Availability of copies, and electronic access.

Copies: To order copies of the **Federal Register** containing this document, send your request to: New Orders, Superintendent of Documents, P.O. Box 371954, Pittsburgh, PA 15250–7954. Specify the date of the issue requested and enclose a check or money order payable to the Superintendent of Documents, or enclose your Visa or Master Card number and expiration date. Credit card orders can also be placed by calling the order desk at (202) 512–1800 (or 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 HHS Office for Civil Rights (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 certain 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 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 legislating to protect the confidentiality of health care information. The Secretary submitted such recommendations to Congress on September 11, 1997, but Congress did not pass such legislation 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 HIPAA Administrative Simplification 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 standards if the changes are necessary to permit compliance with the standards. 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 after the adoption of the modification.

B. Regulatory and Other Actions to Date

HHS published a proposed Rule setting forth privacy standards for individually identifiable health information 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, a floor of national protections for the privacy of their most sensitive information—health information. Congress has passed other laws to protect consumers' 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 enable them 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 and misunderstanding about 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 opened the Privacy Rule for additional public comment 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 will soon be updated to reflect the modifications adopted in this final Rule. The revised guidance will be available on the HHS Office for Civil Rights (OCR) Privacy Web site at *http://www.hhs.gov/ocr/hipaa/*.

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.

II. Overview of the March 2002 Notice of Proposed Rulemaking (NPRM)

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 effects certain provisions would have on health care quality and access. On March 27, 2002, in response to these concerns, and pursuant to HIPAA's provisions for modifications to the standards, the Department proposed modifications to the Privacy Rule (67 FR 14776).

The Department proposed to modify the following areas or provisions of the Privacy Rule: consent; uses and disclosures for treatment, payment, and health care operations; notice of privacy practices; 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 for which authorizations are required; and de-identification. In addition to these key areas, the proposal included changes to other provisions where necessary to clarify the Privacy Rule. The Department also included in the proposed Rule a list of technical corrections intended as editorial or typographical corrections to the Privacy Rule.

The proposed modifications collectively were 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 reflected 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. The Department welcomed 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 the Department's interest in having the compliance date for these revisions also be no later than April 14, 2003, the Department solicited public comment on the proposed modifications for only 30 days. As stated above, the proposed modifications addressed 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 believed 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. During the 30-day comment period, the Department received in excess of 11,400 comments.

III. Section-by-Section Description of Final Modifications and Response to Comments

A. Section 164.501—Definitions

1. Marketing

December 2000 Privacy Rule

The Privacy Rule defined ''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. To avoid interfering with, or unnecessarily burdening communications about, treatment or about the benefits and services of health plans and health care providers, the Privacy Rule explicitly excluded two types of communications from the definition of ''marketing:'' (1) 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; and (2) 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 provider or health plan in the course of managing an individual's treatment or recommending an alternative treatment. Thus, a health plan could send its

enrollees a listing of network providers, and a health care provider could refer a patient to a specialist without either an authorization under § 164.508 or having to meet the other special requirements in § 164.514(e) that attach to marketing communications. However, these communications qualified for the exception to the definition of ''marketing'' only if they were made orally or, if in writing, were made without remuneration from a third party. For example, it would not have been marketing for a pharmacy to call a patient about the need to refill a prescription, even if that refill reminder was subsidized by a third party; but it would have been marketing for that same, subsidized refill reminder to be sent to the patient in the mail.

Generally, if a communication was marketing, the Privacy Rule required the covered entity to obtain the individual's authorization to use or disclose protected health information to make the communication. However, the Privacy Rule, at § 164.514(e), permitted the covered entity to make health-related marketing communications without such authorization, provided it complied with certain conditions on the manner in which the communications were made. Specifically, the Privacy Rule permitted 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, without first obtaining an authorization for that use or disclosure of protected health information, if the communication: (1) Identified the covered entity as the party making the communication; (2) identified, if applicable, that the covered entity received direct or indirect remuneration from a third party for making the communication; (3) with the exception of general circulation materials, contained instructions describing how the individual could opt-out of receiving future marketing communications; and (4) where protected health information was used to target the communication about a product or service to individuals based on their health status or health condition, explained why the individual had been targeted and how the product or service related to the health of the individual.

For certain permissible marketing communications, however, the Department did not believe these conditions to be practicable. Therefore, § 164.514(e) also permitted a covered entity to make a marketing communication that occurred in a face-to-face encounter with the individual, or that involved products or services of only nominal value, without meeting the above conditions or requiring an authorization. These provisions, for example, permitted a covered entity to provide sample products during a face-to-face communication, or to distribute calendars, pens, and the like, that displayed the name of a product or provider.

March 2002 NPRM

The Department received many complaints concerning the complexity and unworkability of the Privacy Rule's marketing requirements. Many 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, questions were raised as to whether disease management communications or refill reminders were ''marketing'' communications subject to the special disclosure and opt-out conditions in § 164.514(e). Others stated that it was unclear whether various health care operations activities, such as general health-related educational and wellness promotional activities, were to be treated as marketing under the Privacy Rule.

The Department also learned that consumers were generally dissatisfied with the conditions required by § 164.514(e). Many 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, and from the intrusion of unwanted solicitations. They 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 who affirmatively chose to receive such communications.

In response to these concerns, the Department proposed to modify the Privacy Rule to make the marketing provisions clearer and simpler. First, the Department proposed to simplify the Privacy Rule by eliminating the special provisions for marketing health-related products and services at § 164.514(e). Instead, any use or disclosure of protected health information for a communication defined as ''marketing'' in § 164.501 would require an authorization by the individual. Thus, covered entities would no longer be able to make any type of marketing communications that involved the use or disclosure of protected health information without authorization simply by meeting the disclosure and opt-out conditions in the Privacy Rule. The Department intended to effectuate greater consumer privacy protection by requiring authorization for all uses or disclosures of protected health information for marketing communications, as compared to the disclosure and opt-out conditions of § 164.514(e).

Second, the Department proposed minor clarifications to the Privacy Rule's definition of ''marketing'' at § 164.501. Specifically, the Department proposed 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 retained the substance of the ''marketing'' definition, but changed the language slightly to avoid the implication that in order for a communication to be marketing, the purpose or intent of the covered entity in making such a communication would have to be determined. The simplified language permits the Department to make the determination based on the communication itself.

Third, with respect to the exclusions from the definition of ''marketing'' in § 164.501, the Department proposed to simplify the language to avoid confusion and better conform to other sections of the regulation, particularly in the area of treatment communications. The proposal retained the exclusions for communications about a covered entity's own products and services and about the treatment of the individual. With respect to the exclusion for a communication made ''in the course of managing the treatment of that individual,'' the Department proposed to modify the language to use the terms ''case management'' and ''care coordination'' for that individual. These terms are more consistent with the terms used in the definition of ''health care operations,'' and were intended to clarify the Department's intent.

One substantive change to the definition proposed by the Department was to eliminate the condition on the above exclusions from the definition of ''marketing'' that the covered entity could not receive remuneration from a third party for any written communication. This limitation was not well understood and treated similar communications differently. For

example, a prescription refill reminder was marketing if it was in writing and paid for by a third party, while a refill reminder that was not subsidized, or was made orally, was not marketing. With the proposed elimination of the health-related marketing requirements in § 164.514(e) and the proposed requirement that any marketing communication require an individual's prior written authorization, retention of this condition would have adversely affected a health care provider's ability to make many common health-related communications. Therefore, the Department proposed to eliminate the remuneration prohibition to the exceptions to the definition so as not to interfere with necessary and important treatment and health-related communications between a health care provider and patient.

To reinforce the policy requiring an authorization for most marketing communications, the Department proposed to add a new 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 was expected to result in direct or indirect remuneration to the covered entity from a third party, the Department proposed that the authorization state this fact. As noted above, because a use or disclosure of protected health information for marketing communications required an authorization, the disclosure and opt-out provisions in § 164.514(e) no longer would be necessary and the Department proposed to eliminate them. As in the December 2000 Privacy Rule at § 164.514(e)(2), the proposed modifications at § 164.508(a)(3) excluded from the marketing authorization requirements face-to-face communications made by a covered entity to an individual. The Department proposed to retain this exception so that the marketing provisions would not interfere with the relationship and dialogue between health care providers and individuals. Similarly, the Department proposed to retain the exception to the authorization requirement for a marketing communication that involved products or services of nominal value, but proposed to replace the language with the common business term ''promotional gift of nominal value.''

As noted above, because some of the proposed simplifications were a substitute for § 164.514(e), the Department proposed to eliminate that section, and to make conforming changes to remove references to § 164.514(e) at § 164.502(a)(1)(vi) and in paragraph (6)(v) of the definition of ''health care operations'' in § 164.501.

Overview of Public Comments

The following discussion provides an overview of the public comment received on this proposal. Additional comments received on this issue are discussed below in the section entitled, ''Response to Other Public Comments.''

The Department received generally favorable comment on its proposal to simplify the marketing provisions by requiring authorizations for uses or disclosures of protected health information for marketing communications, instead of the special provisions for health-related products and services at § 164.514(e). Many also supported the requirement that authorizations notify the individual of marketing that results in direct or indirect remuneration to the covered entity from a third party. They argued that for patients to make informed decisions, they must be notified of potential financial conflicts of interest. However, some commenters opposed the authorization requirement for marketing, arguing instead for the disclosure and opt-out requirements at § 164.514(e) or for a one-time, blanket authorization from an individual for their marketing activities.

Commenters were sharply divided on whether the Department had properly defined what is and what is not marketing. Most of those opposed to the Department's proposed definitions objected to the elimination of health-related communications for which the covered entity received remuneration from the definition of ''marketing.'' They argued that these communications would have been subject to the consumer protections in § 164.514(e) but, under the proposal, could be made without any protections at all. The mere presence of remuneration raised conflict of interest concerns for these commenters, who feared patients would be misled into thinking the covered entity was acting solely in the patients' best interest when recommending an alternative medication or treatment. Of particular concern to these commenters was the possibility of a third party, such as a pharmaceutical company, obtaining a health care provider's patient list to market its own products or services directly to the patients under the guise of recommending an ''alternative treatment'' on behalf of the provider. Commenters argued that, even if the parties attempted to cloak the transaction in the trappings of a business associate relationship, when the remuneration flowed from the third party to the covered entity, the transaction was tantamount to selling the patient lists and ought to be considered marketing.

On the other hand, many commenters urged the Department to broaden the categories of communications that are not marketing. Several expressed concern that, under the proposal, they would be unable to send newsletters and other general circulation materials with information about health-promoting activities (*e.g.,* screenings for certain diseases) to their patients or members without an authorization. Health plans were concerned that they would be unable to send information regarding enhancements to health insurance coverage to their members and beneficiaries. They argued, among other things, that they should be excluded from the definition of ''marketing'' because these communications would be based on limited, non-clinical protected health information, and because policyholders benefit and use such information to fully evaluate the mix of coverage most appropriate to their needs. They stated that providing such information is especially important given that individual and market-wide needs, as well as benefit offerings, change over time and by statute. For example, commenters informed the Department that some States now require long-term care insurers to offer new products to existing policyholders as they are brought to market and to allow policyholders to purchase the new benefits through a formal upgrade process. These health plans were concerned that an authorization requirement for routine communications about options and enhancements would take significant time and expense. Some insurers also urged that they be allowed to market other lines of insurance to their health plan enrollees.

A number of commenters urged the Department to exclude any activity that met the definitions of ''treatment,'' ''payment,'' or ''health care operations'' from the definition of ''marketing'' so that they could freely inform customers about prescription discount card and price subsidy programs. Still others wanted the Department to broaden the treatment exception to include all health-related communications between providers and patients.

Final Modifications. The Department adopts the modifications to marketing substantially as proposed in the NPRM, but makes changes to the proposed definition of ''marketing'' and further clarifies one of the exclusions from the definition of ''marketing'' in response to comments on the proposal. The

definition of ''marketing'' is modified to close what commenters characterized as a loophole, that is, the possibility that covered entities, for remuneration, could disclose protected health information to a third party that would then be able to market its own products and services directly to individuals. Also, in response to comments, the Department clarifies the language in the marketing exclusion for communications about a covered entity's own products and services.

As it proposed to do, the Department eliminates the special provisions for marketing health-related products and services at § 164.514(e). Except as provided for at § 164.508(a)(3), a covered entity must have the individual's prior written authorization to use or disclose protected health information for marketing communications and will no longer be able to do so simply by meeting the disclosure and opt-out provisions, previously set forth in § 164.514(e). The Department agrees with commenters that the authorization provides individuals with more control over whether they receive marketing communications and better privacy protections for such uses and disclosures of their health information. In response to commenters who opposed this proposal, the Department does not believe that an opt-out requirement for marketing communications would provide a sufficient level of control for patients regarding their health information. Nor does the Department believe that a blanket authorization provides sufficient privacy protections for individuals. Section 164.508(c) sets forth the core elements of an authorization necessary to give individuals control of their protected health information. Those requirements give individuals sufficient information and notice regarding the type of use or disclosure of their protected health information that they are authorizing. Without such specificity, an authorization would not have meaning. Indeed, blanket marketing authorizations would be considered defective under § 164.508(b)(2).

The Department adopts the general definition of ''marketing'' with one clarification. Thus, ''marketing'' means ''to make a communication about a product or service that encourages the recipients of the communication to purchase or use the product or service.'' In removing the language referencing the purpose of the communication and substituting the term ''that encourages'' for the term ''to encourage'', the Department intends to simplify the determination of whether a communication is marketing. If, on its face, the communication encourages recipients of the communication to purchase or use the product or service, the communication is marketing. A few commenters argued for retaining the purpose of the communication as part of the definition of ''marketing'' based on their belief that the intent of the communication was a clearer and more definitive standard than the effect of the communication. The Department disagrees with these commenters. Tying the definition of ''marketing'' to the purpose of the communication creates a subjective standard that would be difficult to enforce because the intent of the communicator rarely would be documented in advance. The definition adopted by the Secretary allows the communication to speak for itself.

The Department further adopts the three categories of communications that were proposed as exclusions from the definition of ''marketing.'' Thus, the covered entity is not engaged in marketing when it communicates to individuals about: (1) The participating providers and health plans in a network, the services offered by a provider, or the benefits covered by a health plan; (2) the individual's treatment; or (3) case management or care coordination for that individual, or directions or recommendations for alternative treatments, therapies, health care providers, or settings of care to that individual. For example, a doctor that writes a prescription or refers an individual to a specialist for follow-up tests is engaging in a treatment communication and is not marketing a product or service. The Department continues to exempt from the ''marketing'' definition the same types of communications that were not marketing under the Privacy Rule as published in December 2000, but has modified some of the language to better track the terminology used in the definition of ''health care operations.'' The commenters generally supported this clarification of the language.

The Department, however, does not agree with commenters that sought to expand the exceptions from marketing for all communications that fall within the definitions of ''treatment,'' ''payment,'' or ''health care operations.'' The purpose of the exclusions from the definition of marketing is to facilitate those communications that enhance the individual's access to quality health care. Beyond these important communications, the public strongly objected to any commercial use of protected health information to attempt to sell products or services, even when the product or service is arguably health related. In light of these strong public objections, ease of administration is an insufficient justification to categorically exempt all communications about payment and health care operations from the definition of ''marketing.''

However, in response to comments, the Department is clarifying the language that excludes from the definition of ''marketing'' those communications that describe network participants and the services or benefits of the covered entity. Several commenters, particularly insurers, were concerned that the reference to a ''plan of benefits'' was too limiting and would prevent them from sending information to their enrollees regarding enhancements or upgrades to their health insurance coverage. They inquired whether the following types of communications would be permissible: enhancements to existing products; changes in deductibles/copays and types of coverage (e.g., prescription drug); continuation products for students reaching the age of majority on parental policies; special programs such as guaranteed issue products and other conversion policies; and prescription drug card programs. Some health plans also inquired if they could communicate with beneficiaries about ''one-stop shopping'' with their companies to obtain long-term care, property, casualty, and life insurance products.

The Department understands the need for covered health care providers and health plans to be able to communicate freely to their patients or enrollees about their own products, services, or benefits. The Department also understands that some of these communications are required by State or other law. To ensure that such communications may continue, the Department is broadening its policy, both of the December 2000 Privacy Rule as well as proposed in the March 2002 NPRM, to allow covered entities to use protected health information to convey information to beneficiaries and members about health insurance products offered by the covered entity that could enhance or substitute for existing health plan coverage. Specifically, the Department modifies the relevant exemption from the definition of ''marketing'' to include communications that describe ''a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a

health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits.'' Thus, under this exemption, a health plan is not engaging in marketing when it advises its enrollees about other available health plan coverages that could enhance or substitute for existing health plan coverage. For example, if a child is about to age out of coverage under a family's policy, this provision will allow the plan to send the family information about continuation coverage for the child. This exception, however, does not extend to excepted benefits (described in section 2791(c)(1) of the Public Health Service Act, 42 U.S.C. 300gg–91(c)(1)), such as accident-only policies), nor to other lines of insurance (*e.g.,* it is marketing for a multi-line insurer to promote its life insurance policies using protected health information).

Moreover, the expanded language makes clear that it is not marketing when a health plan communicates about health-related products and services available only to plan enrollees or members that add value to, but are not part of, a plan of benefits. The provision of value-added items or services (VAIS) is a common practice, particularly for managed care organizations. Communications about VAIS may qualify as a communication that is about a health plan's own products or services, even if VAIS are not considered plan benefits for the Adjusted Community Rate purposes. To qualify for this exclusion, however, the VAIS must meet two conditions. First, they must be health-related. Therefore, discounts offered by Medicare+Choice or other managed care organizations for eyeglasses may be considered part of the plan's benefits, whereas discounts to attend movie theaters will not. Second, such items and services must demonstrably ''add value'' to the plan's membership and not merely be a pass-through of a discount or item available to the public at large. Therefore, a Medicare+Choice or other managed care organization could, for example, offer its members a special discount opportunity for a health/fitness club without obtaining authorizations, but could not pass along to its members discounts to a health fitness club that the members would be able to obtain directly from the health/fitness clubs.

In further response to comments, the Department has added new language to the definition of ''marketing'' to close what commenters perceived as a loophole that a covered entity could sell protected health information to another company for the marketing of that company's products or services. For example, many were concerned that a pharmaceutical company could pay a provider for a list of patients with a particular condition or taking a particular medication and then use that list to market its own drug products directly to those patients. The commenters believed the proposal would permit this to happen under the guise of the pharmaceutical company acting as a business associate of the covered entity for the purpose of recommending an alternative treatment or therapy to the individual. The Department agrees with commenters that the potential for manipulating the business associate relationship in this fashion should be expressly prohibited. Therefore, the Department is adding language that would make clear that business associate transactions of this nature are marketing. Marketing is defined expressly to include ''an arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.'' These communications are marketing and can only occur if the covered entity obtains the individual's authorization pursuant to § 164.508. The Department believes that this provision will make express the fundamental prohibition against covered entities selling lists of patients or enrollees to third parties, or from disclosing protected health information to a third party for the marketing activities of the third party, without the written authorization of the individual. The Department further notes that manufacturers that receive identifiable health information and misuse it may be subject to action taken under other consumer protection statutes by other Federal agencies, such as the Federal Trade Commission.

The Department does not, however, agree with commenters who argued for retention of the provisions that would condition the exclusions from the ''marketing'' definition on the absence of remuneration. Except for the arrangements that are now expressly defined as ''marketing,'' the Department eliminates the conditions that communications are excluded from the definition of ''marketing'' only if they are made orally, or, if in writing, are made without any direct or indirect remuneration. The Department does not agree that the simple receipt of remuneration should transform a treatment communication into a commercial promotion of a product or service. For example, health care providers should be able to, and can, send patients prescription refill reminders regardless of whether a third party pays or subsidizes the communication. The covered entity also is able to engage a legitimate business associate to assist it in making these permissible communications. It is only in situations where, in the guise of a business associate, an entity other than the covered entity is promoting its own products using protected health information it has received from, and for which it has paid, the covered entity, that the remuneration will place the activity within the definition of ''marketing.''

In addition, the Department adopts the proposed marketing authorization provision at § 164.508(a)(3), with minor language changes to conform to the revised ''marketing'' definition. The Rule expressly requires an authorization for uses or disclosures of protected health information for marketing communications, except in two circumstances: (1) When the communication occurs in a face-to-face encounter between the covered entity and the individual; or (2) the communication involves a promotional gift of nominal value. A marketing authorization must include a statement about remuneration, if any. For ease of administration, the Department has changed the regulatory provision to require a statement on the authorization whenever the marketing ''involves'' direct or indirect remuneration to the covered entity from a third party, rather than requiring the covered entity to identify those situations where ''the marketing is expected to result in'' remuneration.

Finally, the Department clarifies that nothing in the marketing provisions of the Privacy Rule are to be construed as amending, modifying, or changing any rule or requirement related to any other Federal or State statutes or regulations, including specifically anti-kickback, fraud and abuse, or self-referral statutes or regulations, or to authorize or permit any activity or transaction currently proscribed by such statutes and regulations. Examples of such laws include the anti-kickback statute (section 1128B(b) of the Social Security Act), safe harbor regulations (42 CFR part 1001), Stark law (section 1877 of the Social Security Act) and regulations (42 CFR parts 411 and 424), and HIPAA statute on self-referral (section 1128C of the Social Security Act). The definition

of ''marketing'' is solely applicable to the Privacy Rule and the permissions granted by the Rule are only for a covered entity's use or disclosure of protected health information. In particular, although this regulation defines the term ''marketing'' to exclude communications to an individual to recommend, purchase, or use a product or service as part of the treatment of the individual or for case management or care coordination of that individual, such communication by a ''white coat'' health care professional may violate the anti-kickback statute. Similar examples for pharmacist communications with patients relating to the marketing of products on behalf of pharmaceutical companies were identified by the OIG as problematic in a 1994 Special Fraud Alert (December 19, 1994, 59 FR 65372). Other violations have involved home health nurses and physical therapists acting as marketers for durable medical equipment companies. Although a particular communication under the Privacy Rule may not require patient authorization because it is not marketing, or may require patient authorization because it is ''marketing'' as the Rule defines it, the arrangement may nevertheless violate other statutes and regulations administered by HHS, the Department of Justice, or other Federal or State agency.

Response to Other Public Comments

Comment: Some commenters recommended that the definition of ''marketing'' be broadened to read as follows: ''any communication about a product or service to encourage recipients of the communication to purchase or use the product or service or that will make the recipient aware of the product or service available for purchase or use by the recipient.'' According to these commenters, the additional language would capture marketing campaign activities to establish ''brand recognition.''

Response: The Department believes that marketing campaigns to establish brand name recognition of products is already encompassed within the general definition of ''marketing'' and that it is not necessary to add language to accomplish this purpose.

Comment: Some commenters opposed the proposed deletion of references to the covered entity as the source of the communications, in the definition of those communications that were excluded from the ''marketing'' definition. They objected to these non-marketing communications being made by unrelated third parties based on protected health information disclosed to these third parties by the covered entity, without the individual's knowledge or authorization.

Response: These commenters appear to have misinterpreted the proposal as allowing third parties to obtain protected health information from covered entities for marketing or other purposes for which the Rule requires an individual's authorization. The deletion of the specific reference to the covered entity does not permit disclosures to a third party beyond the disclosures already permitted by the Rule. The change is intended to be purely editorial: since the Rule applies only to covered entities, the only entities whose communications can be governed by the Rule are covered entities, and thus the reference to covered entities there was redundant. Covered entities may not disclose protected health information to third parties for marketing purposes without authorization from the individual, even if the third party is acting as the business associate of the disclosing covered entity. Covered entities may, however, use protected health information to communicate with individuals about the covered entity's own health-related products or services, the individual's treatment, or case management or care coordination for the individual. The covered entity does not need an authorization for these types of communications and may make the communication itself or use a business associate to do so.

Comment: Some commenters advocated for reversion to the provision in § 164.514(e) that the marketing communication identify the covered entity responsible for the communication, and argued that the covered entity should be required to identify itself as the source of the protected health information.

Response: As modified, the Privacy Rule requires the individual's written authorization for the covered entity to use or disclose protected health information for marketing purposes, with limited exceptions. The Department believes that the authorization process itself will put the individual sufficiently on notice that the covered entity is the source of the protected health information. To the extent that the commenter suggests that these disclosures are necessary for communications that are not ''marketing'as defined by the Rule, the Department disagrees because such a requirement would place an undue burden on necessary health-related communications.

Comment: Many commenters opposed the proposed elimination of the provision that would have transformed a communication exempted from marketing into a marketing communication if it was in writing and paid for by a third party. They argued that marketing should include any activity in which a covered entity receives compensation, directly or indirectly, through such things as discounts from another provider, manufacturer, or service provider in exchange for providing information about the manufacturer or service provider's products to consumers, and that consumers should be advised whenever such remuneration is involved and allowed to opt-out of future communications.

Response: The Department considered whether remuneration should determine whether a given activity is marketing, but ultimately concluded that remuneration should not define whether a given activity is marketing or falls under an exception to marketing. In fact, the Department believes that the provision in the December 2000 Rule that transformed a treatment communication into a marketing communication if it was in writing and paid for by a third party blurred the line between treatment and marketing in ways that would have made the Privacy Rule difficult to implement. The Department believes that certain health care communications, such as refill reminders or informing patients about existing or new health care products or services, are appropriate, whether or not the covered entity receives remuneration from third parties to pay for them. The fact that remuneration is received for a marketing communication does not mean the communication is biased or inaccurate. For the same reasons, the Department does not believe that the communications that are exempt from the definition of ''marketing'' require any special conditions, based solely on direct or indirect remuneration received by the covered entity. Requiring disclosure and opt-out conditions on these communications, as § 164.514(e) had formerly imposed on health-related marketing communications, would add a layer of complexity to the Privacy Rule that the Department intended to eliminate. Individuals, of course, are free to negotiate with covered entities for limitations on such uses and disclosures, to which the entity may, but is not required to, agree.

The Department does agree with commenters that, in limited circumstances, abuses can occur. The Privacy Rule, both as published in December 2000 and as proposed to be modified in March 2002, has always prohibited covered entities from selling protected health information to a third

party for the marketing activities of the third party, without authorization. Nonetheless, in response to continued public concern, the Department has added a new provision to the definition of ''marketing'' to prevent situations in which a covered entity could take advantage of the business associate relationship to sell protected health information to another entity for that entity's commercial marketing purposes. The Department intends this prohibition to address the potential financial conflict of interest that would lead a covered entity to disclose protected health information to another entity under the guise of a treatment exemption.

Comment: Commenters argued that written authorizations (opt-ins) should be required for the use of clinical information in marketing. They stated that many consumers do not want covered entities to use information about specific clinical conditions that an individual has, such as AIDS or diabetes, to target them for marketing of services for such conditions.

Response: The Department does not intend to interfere with the ability of health care providers or health plans to deliver quality health care to individuals. The ''marketing'' definition excludes communications for the individual's treatment and for case management, care coordination or the recommendation of alternative therapies. Clinical information is critical for these communications and, hence, cannot be used to distinguish between communications that are or are not marketing. The covered entity needs the individual's authorization to use or disclose protected health information for marketing communications, regardless of whether clinical information is to be used.

Comment: The proposed modification eliminated the § 164.514 requirements that permitted the use of protected health information to market health-related products and services without an authorization. In response to that proposed modification, many commenters asked whether covered entities would be allowed to make communications about ''health education'' or ''health promoting'' materials or services without an authorization under the modified Rule. Examples included communications about health improvement or disease prevention, new developments in the diagnosis or treatment of disease, health fairs, health/wellness-oriented classes or support groups.

Response: The Department clarifies that a communication that merely promotes health in a general manner and does not promote a specific product or service from a particular provider does not meet the general definition of ''marketing.'' Such communications may include population-based activities to improve health or reduce health care costs as set forth in the definition of ''health care operations'' at § 164.501. Therefore, communications, such as mailings reminding women to get an annual mammogram, and mailings providing information about how to lower cholesterol, about new developments in health care (e.g., new diagnostic tools), about health or ''wellness'' classes, about support groups, and about health fairs are permitted, and are not considered marketing.

Comment: Some commenters asked whether they could communicate with beneficiaries about government programs or government-sponsored programs such as information about SCHIP; eligibility for Medicare/Medigap (e.g., eligibility for limited, six-month open enrollment period for Medicare supplemental benefits).

Response: The Department clarifies that communications about government and government-sponsored programs do not fall within the definition of ''marketing.'' There is no commercial component to communications about benefits available through public programs. Therefore, a covered entity is permitted to use and disclose protected health information to communicate about eligibility for Medicare supplemental benefits, or SCHIP. As in our response above, these communications may reflect population-based activities to improve health or reduce health care costs as set forth in the definition of ''health care operations'' at § 164.501.

Comment: The proposed modification eliminated the § 164.514 requirements that allowed protected health information to be used and disclosed without authorization or the opportunity to opt-out, for communications contained in newsletters or similar general communication devices widely distributed to patients, enrollees, or other broad groups of individuals. Many commenters requested clarification as to whether various types of general circulation materials would be permitted under the proposed modification. Commenters argued that newsletters or similar general communication devices widely distributed to patients, enrollees, or other broad groups of individuals should be permitted without authorizations because they are ''common'' and ''serve appropriate information distribution purposes'' and, based on their general circulation, are less intrusive than other forms of communication.

Response: Covered entities may make communications in newsletter format without authorization so long as the content of such communications is not ''marketing,'' as defined by the Rule. The Department is not creating any special exemption for newsletters.

Comment: One commenter suggested that, even when authorizations are granted to disclose protected health information for a particular marketing purpose to a non-covered entity, there should also be an agreement by the third party not to re-disclose the protected health information. This same commenter also recommended that the Privacy Rule place restrictions on non-secure modes of making communications pursuant to an authorization. This commenter argued that protected health information should not be disclosed on the outside of mailings or through voice mail, unattended FAX, or other modes of communication that are not secure.

Response: Under the final Rule, a covered entity must obtain an individual's authorization to use or disclose protected health information for a marketing communication, with some exceptions. If an individual wanted an authorization to limit the use of the information by the covered entity, the individual could negotiate with the covered entity to make that clear in the authorization. Similarly, individuals can request confidential forms of communication, even with respect to authorized disclosures. See § 164.522(b).

Comment: Commenters requested that HHS provide clear guidance on what types of activities constitute a use or disclosure for marketing, and, therefore, require an authorization.

Response: The Department has modified the ''marketing'' definition to clarify the types of uses or disclosures of protected health information that are marketing, and, therefore, require prior authorization and those that are not marketing. The Department intends to update its guidance on this topic and address specific examples raised by commenters at that time.

Comment: A number of commenters wanted the Department to amend the face-to-face authorization exception. Some urged that it be broadened to include telephone, mail and other common carriers, fax machines, or the Internet so that the exception would cover communications between providers and patients that are not in person. For example, it was pointed out that some providers, such as home

delivery pharmacies, may have a direct treatment relationship, but communicate with patients through other channels. Some raised specific concerns about communicating with ''shut-ins'' and ''persons living in rural areas.'' Other commenters asked the Department to make the exception more narrow to cover only those marketing communications made by a health care provider, as opposed to by a business associate, or to cover only those marketing communications of a provider that arise from a treatment or other essential health care communication.

Response: The Department believes that expanding the face-to-face authorization exception to include telephone, mail, and other common carriers, fax machines or the Internet would create an exception essentially for all types of marketing communications. All providers potentially use a variety of means to communicate with their patients. The authorization exclusion, however, is narrowly crafted to permit only face-to-face encounters between the covered entity and the individual.

The Department believes that further narrowing the exception to place conditions on such communications, other than that it be face-to-face, would neither be practical nor better serve the privacy interests of the individual. The Department does not intend to police communications between doctors and patients that take place in the doctor's office. Further limiting the exception would add a layer of complexity to the Rule, encumbering physicians and potentially causing them to second-guess themselves when making treatment or other essential health care communications. In this context, the individual can readily stop any unwanted communications, including any communications that may otherwise meet the definition of ''marketing.''

2. Health Care Operations: Changes of Legal Ownership

December 2000 Privacy Rule. The Rule's definition of ''health care operations'' included the disclosure of protected health information for the purposes of due diligence with respect to the contemplated sale or transfer of all or part of a covered entity's assets to a potential successor in interest who is a covered entity, or would become a covered entity as a result of the transaction.

The Department indicated in the December 2000 preamble of the Privacy Rule its intent to include in the definition of health care operations the actual transfer of protected health information to a successor in interest upon a sale or transfer of its assets. (65 FR 82609.) However, the regulation itself did not expressly provide for the transfer of protected health information upon the sale or transfer of assets to a successor in interest. Instead, the definition of ''health care operations'' included uses or disclosures of protected health information only for due diligence purposes when a sale or transfer to a successor in interest is contemplated.

March 2002 NPRM. A number of entities expressed concern about the discrepancy between the intent as expressed in the preamble to the December 2000 Privacy Rule and the actual regulatory language. To address these concerns, the Department proposed to add language to paragraph (6) of the definition of ''health care operations'' to clarify its 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 proposed to use the terms ''sale, transfer, consolidation or merger'' and 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 believed the current language may not accomplish this goal.

The Department proposed to retain 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 would become a covered entity as a result of the transaction. The Department clarified that the proposed modification would not affect a covered entity's other legal or ethical obligation to notify individuals of a sale, transfer, merger, or consolidation.

Overview of Public Comments. The following discussion provides an overview of the public comment received on this proposal. Additional comments received on this issue are discussed below in the section entitled, ''Response to Other Public Comments.''

Numerous commenters supported the proposed modifications. Generally, these commenters claimed the modifications would prevent inconvenience to consumers, and facilitate timely access to health care. Specifically, these commenters indicated that health care would be delayed and consumers would be inconvenienced if covered entities were required to obtain individual consent or authorization before they could access health records that are newly acquired assets resulting from the sale, transfer, merger, or consolidation of all or part of a covered entity. Commenters further claimed that the administrative burden of acquiring individual permission and culling records of consumers who do not give consent would be too great, and would cause some entities to simply store or destroy the records instead. Consequently, health information would be inaccessible, causing consumers to be inconvenienced and health care to be delayed. Some commenters noted that the proposed modifications recognize the realities of business without compromising the availability or quality of health care or diminishing privacy protections one would expect in the handling of protected health information during the course of such business transactions.

Opposition to the proposed modifications was limited, with commenters generally asserting that the transfer of records in such circumstances would not be in the best interests of individuals.

Final Modifications. The Department agrees with the commenters that supported the proposed modifications and, therefore, adopts the modifications to the definition of health care operations. Thus, ''health care operations'' includes the sale, transfer, merger, or consolidation of all or part of the covered entity to or with another covered entity, or an entity that will become a covered entity as a result of the transaction, as well as the due diligence activities in connection with such transaction. In response to a comment, the final Rule modifies the phrase ''all or part of a covered entity'' to read ''all or part of the covered entity'' to clarify that any disclosure for such activity must be by the covered entity that is a party to the transaction.

Under the final definition of ''health care operations,'' a covered entity may use or disclose protected health information in connection with a sale or transfer of assets to, or a consolidation or merger with, an entity that is or will be a covered entity upon completion of the transaction; and to conduct due diligence in connection with such transaction. The modification makes clear it is also a health care operation to transfer records containing protected health information as part of the transaction. For example, if a pharmacy which is a covered entity buys another pharmacy which is also a covered entity, protected health information can be exchanged between the two entities for purposes of conducting due diligence, and the selling entity may

transfer any records containing protected health information to the new owner upon completion of the transaction. The new owner may then immediately use and disclose those records to provide health care services to the individuals, as well as for payment and health care operations purposes. Since the information would continue to be protected by the Privacy Rule, any other use or disclosure of the information would require an authorization unless otherwise permitted without authorization by the Rule, and the new owner would be obligated to observe the individual's rights of access, amendment, and accounting. The Privacy Rule would not interfere with other legal or ethical obligations of an entity that may arise out of the nature of its business or relationship with its customers or patients to provide such persons with notice of the transaction or an opportunity to agree to the transfer of records containing personal information to the new owner.

Response to Other Public Comments

Comment: One commenter was concerned about what obligations the parties to a transaction have regarding protected health information that was exchanged as part of a transaction if the transaction does not go through.

Response: The Department believes that other laws and standard business practices are adequate to address these situations and accordingly does not impose additional requirements of this type. It is standard practice for parties contemplating such transactions to enter into confidentiality agreements. In addition to exchanging protected health information, the parties to such transactions commonly exchange confidential proprietary information. It is a standard practice for the parties to these transaction to agree that the handling of all confidential information, such as proprietary information, will include ensuring that, in the event that the proposed transaction is not consummated, the information is either returned to its original owner or destroyed as appropriate. They may include protected health information in any such agreement, as they determine appropriate to the circumstances and applicable law.

3. Protected Health Information: Exclusion for Employment Records

December 2000 Privacy Rule. The Privacy Rule broadly defines ''protected health information'' as individually identifiable health information maintained or transmitted by a covered entity in any form or medium. The December 2000 Privacy Rule expressly excluded from the definition of ''protected health information'' only educational and other records that are covered by the Family Education Rights and Privacy Act of 1974, as amended, 20 U.S.C. 1232g. In addition, throughout the December 2000 preamble to the Privacy Rule, the Department repeatedly stated that the Privacy Rule does not apply to employers, nor does it apply to the employment functions of covered entities, that is, when they are acting in their role as employers. For example, the Department stated:

> Covered entities must comply with this regulation in their health care capacity, not in their capacity as employers. For example, information in hospital personnel files about a nurses' (sic) sick leave is not protected health information under this rule.

65 FR 82612. However, the definition of protected health information did not expressly exclude personnel or employment records of covered entities.

March 2002 NPRM. The Department understands that covered entities are also employers, and that this creates two potential sources of confusion about the status of health information. First, some employers are required or elect to obtain health information about their employees, as part of their routine employment activities [e.g., hiring, compliance with the Occupational Safety and Health Administration (OSHA) requirements]. Second, employees of covered health care providers or health plans sometimes seek treatment or reimbursement from that provider or health plan, unrelated to the employment relationship.

To avoid any confusion on the part of covered entities as to application of the Privacy Rule to the records they maintain as employers, the Department proposed to modify the definition of ''protected health information'' in § 164.501 to expressly exclude employment records held by a covered entity in its role as employer. The proposed modification also would alleviate the situation where a covered entity would feel compelled to elect to designate itself as a hybrid entity solely to carve out its employment functions. Individually identifiable health information maintained or transmitted by a covered entity in its health care capacity would, under the proposed modification, continue to be treated as protected health information.

The Department specifically solicited comments on whether the term ''employment records'' is clear and what types of records would be covered by the term.

In addition, as discussed in section III.C.1. below, the Department proposed to modify the definition of a hybrid entity to permit any covered entity that engaged in both covered and non-covered functions to elect to operate as a hybrid entity. Under the proposed modification, a covered entity that primarily engaged in covered functions, such as a hospital, would be allowed to elect hybrid entity status even if its only non-covered functions were those related to its capacity as an employer. Indeed, because of the absence of an express exclusion for employment records in the definition of protected health information, some covered entities may have elected hybrid entity status under the misconception that this was the only way to prevent their personnel information from being treated as protected health information under the Rule.

Overview of Public Comments. The following discussion provides an overview of the public comment received on this proposal. Additional comments received on this issue are discussed below in the section entitled, ''Response to Other Public Comments.''

The Department received comments both supporting and opposing the proposal to add an exemption for employment records to the definition of protected health information. Support for the proposal was based primarily on the need for clarity and certainty in this important area. Moreover, commenters supported the proposed exemption for employment records because it reinforced and clarified that the Privacy Rule does not conflict with an employer's obligation under numerous other laws, including OSHA, Family and Medical Leave Act (FMLA), workers' compensation, and alcohol and drug free workplace laws.

Those opposed to the modification were concerned that a covered entity may abuse its access to the individually identifiable health information in its employment records by using that information for discriminatory purposes. Many commenters expressed concern that an employee's health information created, maintained, or transmitted by the covered entity in its health care capacity would be considered an employment record and, therefore, would not be considered protected health information. Some of these commenters argued for the inclusion of special provisions, similar to the ''adequate separation'' requirements for disclosure of protected health information from group health plan to plan sponsor functions (§ 164.504(f)), to heighten the protection for an employee's individually identifiable health information when moving between a covered entity's

health care functions and its employer functions.

A number of commenters also suggested types of records that the Department should consider to be ''employment records'' and, therefore, excluded from the definition of ''protected health information.'' The suggested records included records maintained under the FMLA or the Americans with Disabilities Act (ADA), as well as records relating to occupational injury, disability insurance eligibility, sick leave requests and justifications, drug screening results, workplace medical surveillance, and fitness-for-duty test results. One commenter suggested that health information related to professional athletes should qualify as an employment record.

Final Modifications. The Department adopts as final the proposed language excluding employment records maintained by a covered entity in its capacity as an employer from the definition of ''protected health information.'' The Department agrees with commenters that the regulation should be explicit that it does not apply to a covered entity's employer functions and that the most effective means of accomplishing this is through the definition of ''protected health information.''

The Department is sensitive to the concerns of commenters that a covered entity not abuse its access to an employee's individually identifiable health information which it has created or maintains in its health care, not its employer, capacity. In responding to these concerns, the Department must remain within the boundaries set by the statute, which does not include employers per se as covered entities. Thus, we cannot regulate employers, even when it is a covered entity acting as an employer.

To address these concerns, the Department clarifies that a covered entity must remain cognizant of its dual roles as an employer and as a health care provider, health plan, or health care clearinghouse. Individually identifiable health information created, received, or maintained by a covered entity in its health care capacity is protected health information. It does not matter if the individual is a member of the covered entity's workforce or not. Thus, the medical record of a hospital employee who is receiving treatment at the hospital is protected health information and is covered by the Rule, just as the medical record of any other patient of that hospital is protected health information and covered by the Rule. The hospital may use that information only as permitted by the Privacy Rule, and in most cases will need the employee's authorization to access or use the medical information for employment purposes. When the individual gives his or her medical information to the covered entity as the employer, such as when submitting a doctor's statement to document sick leave, or when the covered entity as employer obtains the employee's written authorization for disclosure of protected health information, such as an authorization to disclose the results of a fitness for duty examination, that medical information becomes part of the employment record, and, as such, is no longer protected health information. The covered entity as employer, however, may be subject to other laws and regulations applicable to the use or disclosure of information in an employee's employment record.

The Department has decided not to add a definition of the term ''employment records'' to the Rule. The comments indicate that the same individually identifiable health information about an individual may be maintained by the covered entity in both its employment records and the medical records it maintains as a health care provider or enrollment or claims records it maintains as a health plan. The Department therefore is concerned that a definition of ''employment record'' may lead to the misconception that certain types of information are never protected health information, and will put the focus incorrectly on the nature of the information rather than the reasons for which the covered entity obtained the information. For example, drug screening test results will be protected health information when the provider administers the test to the employee, but will not be protected health information when, pursuant to the employee's authorization, the test results are provided to the provider acting as employer and placed in the employee's employment record. Similarly, the results of a fitness for duty exam will be protected health information when the provider administers the test to one of its employees, but will not be protected health information when the results of the fitness for duty exam are turned over to the provider as employer pursuant to the employee's authorization.

Furthermore, while the examples provided by commenters represent typical files or records that may be maintained by employers, the Department does not believe that it has sufficient information to provide a complete definition of employment record. Therefore, the Department does not adopt as part of this rulemaking a definition of employment record, but does clarify that medical information needed for an employer to carry out its obligations under FMLA, ADA, and similar laws, as well as files or records related to occupational injury, disability insurance eligibility, sick leave requests and justifications, drug screening results, workplace medical surveillance, and fitness-for-duty tests of employees, may be part of the employment records maintained by the covered entity in its role as an employer.

Response to Other Public Comments

Comment: One commenter requested clarification as to whether the term ''employment record'' included the following information that is either maintained or transmitted by a fully insured group health plan to an insurer or HMO for enrollment and/or disenrollment purposes: (a) the identity of an individual including name, address, birth date, marital status, dependent information and SSN; (b) the individual's choice of plan; (c) the amount of premiums/contributions for coverage of the individual; (d) whether the individual is an active employee or retired; (e) whether the individual is enrolled in Medicare.

Response: All of this information is protected health information when held by a fully insured group health plan and transmitted to an issuer or HMO, and the Privacy Rule applies when the group health plan discloses such information to any entity, including the plan sponsor. There are special rules in § 164.504(f) which describe the conditions for disclosure of protected health information to the plan sponsor. If the group health plan received the information from the plan sponsor, it becomes protected health information when received by the group health plan. The plan sponsor is not the covered entity, so this information will not be protected when held by a plan sponsor, whether or not it is part of the plan sponsor's ''employment record.''

Comment: One commenter asked for clarification as to how the Department would characterize the following items that a covered entity may have: (1) medical file kept separate from the rest of an employment record containing (a) doctor's notes; (b) leave requests; (c) physician certifications; and (d) positive hepatitis test results; (2) FMLA documentation including: (a) physician certification form; and (b) leave requests; (3) occupational injury files containing (a) drug screening; (b) exposure test results; (c) doctor's notes; and (d) medical director's notes.

Response: As explained above, the nature of the information does not determine whether it is an employment record. Rather, it depends on whether the covered entity obtains or creates the information in its capacity as employer or in its capacity as covered entity. An employment record may well contain some or all of the items mentioned by the commenter; but so too might a treatment record. The Department also recognizes that the employer may be required by law or sound business practice to treat such medical information as confidential and maintain it separate from other employment records. It is the function being performed by the covered entity and the purpose for which the covered entity has the medical information, not its record keeping practices, that determines whether the health information is part of an employment record or whether it is protected health information.

Comment: One commenter suggested that the health records of professional athletes should qualify as ''employment records.'' As such, the records would not be subject to the protections of the Privacy Rule.

Response: Professional sports teams are unlikely to be covered entities. Even if a sports team were to be a covered entity, employment records of a covered entity are not covered by this Rule. If this comment is suggesting that the records of professional athletes should be deemed ''employment records'' even when created or maintained by health care providers and health plans, the Department disagrees. No class of individuals should be singled out for reduced privacy protections. As noted in the preamble to the December 2000 Rule, nothing in this Rule prevents an employer, such as a professional sports team, from making an employee's agreement to disclose health records a condition of employment. A covered entity, therefore, could disclose this information to an employer pursuant to an authorization.

B. Section 164.502—Uses and Disclosures of Protected Health Information: General Rules

1. Incidental Uses and Disclosures

December 2000 Privacy Rule. The December 2000 Rule did not explicitly address incidental uses and disclosures of protected health information. Rather, the Privacy Rule 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. *See* § 164.502(b). Additionally, § 164.530(c) of the Privacy Rule requires covered entities to implement appropriate administrative, technical, and physical safeguards to reasonably safeguard protected health information from any intentional or unintentional use or disclosure that violates the Rule.

Protected health information includes individually identifiable health information (with limited exceptions) in any form, including information transmitted orally, or in written or electronic form. See the definition of ''protected health information'' at § 164.501.

March 2002 NPRM. After publication of the Privacy Rule, the Department received a number of 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. In particular, concern was expressed that the Privacy Rule establishes absolute, strict standards that would not allow for the incidental or unintentional disclosures that could occur as a by-product of engaging in these health care communications and practices. It was argued that the Privacy Rule would, in effect, prohibit such practices and, therefore, impede many activities and communications essential to effective and timely treatment of patients.

For example, some expressed concern that health care providers could no longer engage in confidential conversations with other providers or with patients, if there is a possibility that they could be overheard. Similarly, others questioned whether they would be prohibited from using sign-in sheets in waiting rooms or maintaining patient charts at bedside, or whether they would need to isolate X-ray lightboards or destroy empty prescription vials. These concerns seemed to stem from a perception that covered entities are 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.

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. The guidance promised that the Department would propose modifications to the Privacy Rule 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 proposed to modify the Privacy Rule to add a new provision at § 164.502(a)(1)(iii) which would explicitly permit certain incidental uses and disclosures that occur as a result of a use or disclosure otherwise permitted by the Privacy Rule. The proposal described an incidental use or disclosure as 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. The Department proposed that an incidental use or disclosure be permissible only to the extent that the covered entity had 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).

Overview of Public Comments. The following discussion provides an overview of the public comment received on this proposal. Additional comments received on this issue are discussed below in the section entitled, ''Response to Other Public Comments.''

The Department received many comments on its proposal to permit certain incidental uses and disclosures, the majority of which expressed strong support for the proposal. Many of these commenters indicated that such a policy would help to ensure that essential health care communications and practices are not chilled by the Privacy Rule. A few commenters opposed the Department's proposal to permit certain incidental uses and disclosures, one of whom asserted that the burden on medical staff to take precautions not to be overheard is minimal compared to the potential harm to patients if incidental disclosures were to be considered permissible.

Final Modifications. In response to the overwhelming support of commenters on this proposal, the Department adopts the proposed provision at § 164.502(a)(1)(iii), explicitly permitting certain incidental uses and disclosures that occur as a by-product of a use or disclosure otherwise permitted under the Privacy Rule. As in the proposal, an incidental use or disclosure is 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). The Department continues to believe, as was stated in the proposed Rule, that so long as reasonable safeguards are employed, the burden of impeding such communications is not outweighed by any benefits that may accrue to individuals' privacy interests.

However, an incidental use or disclosure that occurs as a result of a failure to apply reasonable safeguards or the minimum necessary standard, where required, is not a permissible use or disclosure and, therefore, is a violation of the Privacy Rule. For example, a hospital that permits an employee to have unimpeded access to patients' medical records, where such access is not necessary for the employee to do her job, is not applying the minimum necessary standard and, therefore, any incidental use or disclosure that results from this practice would be an unlawful use or disclosure under the Privacy Rule.

In response to the few comments that opposed the proposal to permit certain incidental uses and disclosures, the Department reiterates that the Privacy Rule must not impede essential health care communications and practices. Prohibiting all incidental uses and disclosures would have a chilling effect on normal and important communications among providers, and between providers and their patients, and, therefore, would negatively affect individuals' access to quality health care. The Department does not intend with this provision to obviate the need for medical staff to take precautions to avoid being overheard, but rather, will only allow incidental uses and disclosures where appropriate precautions have been taken.

The Department clarifies, in response to a comment, that this provision applies, subject to reasonable safeguards and the minimum necessary standard, to an incidental use or disclosure that occurs as a result of any permissible use or disclosure under the Privacy Rule made to any person, and not just to incidental uses and disclosures resulting from treatment communications or only to communications among health care providers or other medical staff. For example, a provider may instruct an administrative staff member to bill a patient for a particular procedure, and may be overheard by one or more persons in the waiting room. Assuming that the provider made reasonable efforts to avoid being overheard and reasonably limited the information shared, an incidental disclosure resulting from such conversation is permissible under the Rule.

In the proposal, the Department did not address whether or not incidental disclosures would need to be included in the accounting of disclosures required by § 164.528. However, one commenter urged the Department to exclude incidental disclosures from the accounting. The Department agrees with this commenter and clarifies that covered entities are not required to include incidental disclosures in an accounting of disclosures provided to the individual pursuant to § 164.528. The Department does not believe such a requirement would be practicable; in many instances, the covered entity may not know that an incidental disclosure occurred. To make this policy clear, the Department includes an explicit exception for such disclosures to the accounting standard at § 164.528(a)(1).

Response to Other Public Comments

Comment: One commenter expressed concern that the requirement reasonably to safeguard protected health information would be problematic because any unintended use or disclosure could arguably demonstrate a failure to ''reasonably safeguard.'' This commenter requested that the Department either delete the language in § 164.530(c)(2)(ii) or modify the language to make clear that the fact that an incidental use or disclosure occurs does not imply that safeguards were not reasonable.

Response: The Department clarifies that the fact that an incidental use or disclosure occurs does not by itself imply that safeguards were not reasonable. However, the Department does not believe that a modification to the proposed language is necessary to express this intent. The language proposed and now adopted at § 164.530(c)(2)(ii) requires only that the covered entity reasonably safeguard protected health information to limit incidental uses or disclosures, not that the covered entity prevent all incidental uses and disclosures. Thus, the Department expects that incidental uses and disclosures will occur and permits such uses and disclosures to the extent the covered entity has in place reasonable safeguards and has applied the minimum necessary standard, where applicable.

Comment: Another commenter requested that the Department clarify its proposal to assure that unintended disclosures will not result in civil penalties.

Response: The Department's authority to impose civil monetary penalties on violations of the Privacy Rule is defined in HIPAA. Specifically, HIPAA added section 1176 to the Social Security Act, which prescribes the Secretary's authority to impose civil monetary penalties. Therefore, in the case of a violation of a disclosure provision in the Privacy Rule, a penalty may not be imposed, among other things, if the person liable for the penalty did not know and, by exercising reasonable diligence would not have known, that such person violated the provision. HIPAA also provides for criminal penalties under certain circumstances, but the Department of Justice, not this Department, has authority for criminal penalties.

Comment: One commenter requested that the Department clarify how covered entities should implement technical and physical safeguards when they do not yet know what safeguards the final Security Rule will require.

Response: Each covered entity should assess the nature of the protected health information it holds, and the nature and scope of its business, and implement safeguards that are reasonable for its particular circumstances. There should be no potential for conflict between the safeguards required by the Privacy Rule and the final Security Rule standards, for several reasons. First, while the Privacy Rule applies to protected health information in all forms, the Security Rule will apply only to electronic health information systems that maintain or transmit individually identifiable health information. Thus, all safeguards for protected health information in oral, written, or other non-electronic forms will be unaffected by the Security Rule. Second, in preparing the final Security Rule, the Department is working to ensure the Security Rule requirements for electronic information systems work ''hand in glove'' with any relevant requirements in the Privacy Rule, including § 164.530.

Comment: One commenter argued that while this new provision is helpful, it does not alleviate covered entities' concerns that routine practices, often beneficial for treatment, will be prohibited by the Privacy Rule. This commenter stated that, for example, specialists provide certain types of therapy to patients in a group setting, and, in some cases, where family members are also present.

Response: The Department reiterates that the Privacy Rule is not intended to impede common health care communications and practices that are essential in providing health care to the individual. Further, the Privacy Rule's new provision permitting certain incidental uses and disclosures is

intended to increase covered entities' confidence that such practices can continue even where an incidental use or disclosure may occur, provided that the covered entity has taken reasonable precautions to safeguard and limit the protected health information disclosed. For example, this provision should alleviate concerns that common practices, such as the use of sign-in sheets and calling out names in waiting rooms will not violate the Rule, so long as the information disclosed is appropriately limited. With regard to the commenters' specific example, disclosure of protected health information in a group therapy setting would be a treatment disclosure, and thus permissible without individual authorization. Further, § 164.510(b) generally permits a covered entity to disclose protected health information to a family member or other person involved in the individual's care. In fact, this section specifically provides that, where the individual is present during a disclosure, the covered entity may disclose protected health information if it is reasonable to infer from the circumstances that the individual does not object to the disclosure. Absent countervailing circumstances, the individual's agreement to participate in group therapy or family discussions is a good basis for such a reasonable inference. As such disclosures are permissible disclosures in and of themselves, they would not be incidental disclosures.

Comment: Some commenters, while in support of permitting incidental uses and disclosures, requested that the Department provide additional guidance in this area by providing additional examples of permitted incidental uses and disclosures and/or clarifying what would constitute ''reasonable safeguards.''

Response: The reasonable safeguards and minimum necessary standards are flexible and adaptable to the specific business needs and circumstances of the covered entity. Given the discretion covered entities have in implementing these standards, it is difficult for the Department to provide specific guidance in this area that is generally applicable to many covered entities. However, the Department intends to provide future guidance through frequently asked questions or other materials in response to specific scenarios that are raised by industry.

2. Minimum Necessary Standard

December 2000 Privacy Rule. The Privacy Rule 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. See § 164.502(b). Protected health information includes individually identifiable health information (with limited exceptions) 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 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 purposes of enforcing this Rule. See § 164.502(b)(2).

The Privacy Rule sets forth requirements for implementing the minimum necessary standard with regard to a covered entity's uses, disclosures, and requests at § 164.514(d). 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. 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 the 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 reasonably to rely on representations from a public official, such as a State workers' compensation official, that the information requested is the minimum necessary for the intended purpose. Similarly, a covered entity is permitted reasonably to rely on the judgment of another covered entity 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).

March 2002 NPRM. The Department proposed a number of minor modifications to the minimum necessary standard to clarify the Department's intent or otherwise conform these provisions to other proposed modifications. First, the Department proposed 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 the separate exception for disclosures made to the individual. Second, to conform to the proposal to eliminate the special authorizations required by the Privacy Rule at § 164.508(d), (e), and (f), the Department proposed to exempt from the minimum necessary standard any uses or disclosures for which the covered entity had received an authorization that meets the requirements of § 164.508, rather than just those authorizations initiated by the individual.

Third, the Department proposed 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 the Department's intent that the minimum necessary requirements be reasonable and flexible to the unique circumstances of the covered entity. In addition, the Department proposed to generally revise the language in § 164.514(d)(1) to be more consistent with the description of standards elsewhere in the Privacy Rule.

Fourth, so that the minimum necessary standard would be applied consistently to requests for, and disclosures of, protected health information, the Department proposed to add a provision to § 164.514(d)(4) 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 corresponding implementation specifications for disclosures. Specifically, for requests not made on a routine and recurring basis, the Department proposed to add the requirement that a covered entity must implement the minimum

necessary standard by developing and implementing criteria designed to limit its request for protected health information to the minimum necessary to accomplish the intended purpose.

Overview of Public Comments. The following discussion provides an overview of the public comment received on this proposal. Additional comments received on this issue are discussed below in the section entitled, ''Response to Other Public Comments.''

The Department received a number of comments on its proposal to exempt from the minimum necessary standard any use or disclosure of protected health information for which the covered entity has received an authorization that meets the requirements of § 164.508. Many commenters supported this proposal. A few commenters generally urged that the minimum necessary standard be applied to uses and disclosures pursuant to an authorization. A few other commenters appeared to misinterpret the policy in the December 2000 Rule and urged that the Department retain the minimum necessary standard for disclosures ''pursuant to an authorization other than disclosures to an individual.'' Some commenters raised specific concerns about authorizations for psychotherapy notes and the particular need for minimum necessary to be applied in these cases.

A number of commenters expressed support for the Department's statements in the preamble to the proposed Rule reinforcing that the minimum necessary standard is intended to be flexible to account for the characteristics of the entity's business and workforce, and not intended to override the professional judgment of the covered entity. Similarly, some commenters expressed support for the Department's proposal to remove the term ''reasonably ensure'' from § 164.514(d)(1). However, a few commenters expressed concerns that the proposed alternative language actually would implement a stricter standard than that included in the December 2000 Privacy Rule.

Final Modifications. In this final Rule, the Department adopts the proposed policy to 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 final modification adopts the proposal to eliminate the special authorizations that were required by the December 2000 Privacy Rule at § 164.508(d), (e), and (f). (*See* section III.E.1. of the preamble for a detailed discussion of the modifications to the authorization requirements of the Privacy Rule.) Since the only authorizations to which the minimum necessary standard applied are being eliminated in favor of a single consolidated authorization, the final Rule correspondingly eliminates the minimum necessary provisions that applied to the now-eliminated special authorizations. All uses and disclosures made pursuant to any authorization are exempt from the minimum necessary standard.

In response to commenters who opposed this proposal as a potential weakening of privacy protections or who wanted the minimum necessary requirements to apply to authorizations other than disclosures to the individual, the Department notes that nothing in the final Rule eliminates an individual's control over his or her protected health information with respect to an authorization. All authorizations must include a description of the information to be used and disclosed that identifies the information in a specific and meaningful fashion as required by § 164.508(c)(1)(i). If the individual does not wish to release the information requested, the individual has the right to not sign the authorization or to negotiate a narrower authorization with the requestor.

Additionally, in response to those commenters who raised specific concerns with respect to authorizations which request release of psychotherapy notes, the Department clarifies that the final Rule does not require a covered entity to use and disclose protected health information pursuant to an authorization. Rather, as with most other uses and disclosures under the Privacy Rule, this is only a permissible use or disclosure. If a covered health care provider is concerned that a request for an individual's psychotherapy notes is not warranted or is excessive, the provider may consult with the individual to determine whether or not the authorization is consistent with the individual's wishes.

Further, the Privacy Rule does not permit a health plan to condition enrollment, eligibility for benefits, or payment of a claim on obtaining the individual's authorization to use or disclose psychotherapy notes. Nor may a health care provider condition treatment on an authorization for the use or disclosure of psychotherapy notes. Thus, the Department believes that these additional protections appropriately and effectively protect an individual's privacy with respect to psychotherapy notes.

The final Rule also retains for clarity the proposal to separate § 164.502(b)(2)(ii) into two subparagraphs (§ 164.502(b)(2)(ii) and (iii)); commenters did not explicitly address or raise issues with this proposed clarification.

In response to concerns that the proposed language at § 164.514(d)(1) would implement a stricter standard, the Department disagrees and, therefore, adopts the proposed language. The language in § 164.514(d)(1) describes the standard: covered entities are required to meet the requirements in the implementation specifications of § 164.514(d)(2) through (d)(5). The implementation specifications describe what covered entities must do reasonably to limit uses, disclosures, and requests to the minimum necessary. Thus, the Department believes that the language in the implementation specifications is adequate to reflect the Department's intent that the minimum necessary standard is reasonable and flexible to accommodate the unique circumstances of the covered entity.

Commenters also generally did not address the Department's proposed clarification to make the implementation specifications for requests of protected health information consistent with those for disclosures of protected health information. Consequently, as commenters did not raise concerns with the proposal, this final Rule adopts the proposed provision at § 164.514(d)(4). For requests of protected health information not made on a routine and recurring basis, a covered entity must implement the minimum necessary standard by developing and implementing criteria designed to limit its request for protected health information to the minimum necessary to accomplish the intended purpose.

Response to Other Public Comments

Comment: Many commenters recommended changes to the minimum necessary standard unrelated to the proposed modifications. For example, some commenters urged that the Department exempt from the minimum necessary standard all uses of protected health information, or at least uses of protected health information for treatment purposes. Alternatively, one commenter urged that the minimum necessary standard be applied to disclosures for treatment purposes. Others requested that the Department exempt uses and disclosures for payment and health care operations from the standard, or exempt disclosures to another covered entity for such purposes. A few commenters argued that the minimum necessary standard should not apply to disclosures to another covered entity. Some urged that the minimum

necessary standard be eliminated entirely.

Response: The Department did not propose modifications relevant to these comments, nor did it seek comment on these issues. The proposed modifications generally were intended to address those problems or issues that presented workability problems for covered entities or otherwise had the potential to impede an individual's timely access to quality health care. Moreover, the proposed modifications to the minimum necessary standard were either minor clarifications of the Department's intent with respect to the standard or would conform the standard to other proposed modifications. The Department has, in previous guidance as well as in the preamble to the December 2000 Privacy Rule, explained its position with respect to the above concerns. The minimum necessary standard is derived from confidentiality codes and practices in common use today. We continue to believe that it is sound practice not to use or disclose private medical information that is not necessary to satisfy a request or effectively carry out a function. The privacy benefits of retaining the minimum necessary standard outweigh the burden involved with implementing the standard. The Department reiterates that position here.

Further, the Department designed the minimum necessary standard to be sufficiently flexible to accommodate the various circumstances of any covered entity. Covered entities will develop their own policies and procedures to meet this standard. A covered entity's policies and procedures may and should allow the appropriate individuals within an entity to have access to protected health information as necessary to perform their jobs with respect to the entity's covered functions. The Department is not aware of any workability issues with this standard.

With respect to disclosures to another covered entity, the Privacy Rule permits a covered entity reasonably to rely on another covered entity's request for protected health information as the minimum necessary for the intended disclosure. See § 164.514(d)(3)(iii). The Department does not believe, therefore, that a blanket exception for such disclosures is justified. The covered entity who holds the information always retains discretion to make its own minimum necessary determination.

Lastly, the Department continues to believe that the exception for disclosures to or requests by health care providers for treatment purposes is appropriate to ensure that access to timely and quality treatment is not impeded.

As the Privacy Rule is implemented, the Department will monitor the workability of the minimum necessary standard and consider proposing revisions, where appropriate, to ensure that the Privacy Rule does not hinder timely access to quality health care.

Comment: One commenter requested that the Department state in the preamble that the minimum necessary standard may not be used to interfere with or obstruct essential health plan payment and health care operations activities, including quality assurance, disease management, and other activities. Another commenter asked that the final Rule's preamble acknowledge that, in some cases, the minimum protected health information necessary for payment or health care operations will be the entire record. One commenter urged that the Rule be modified to presume that disclosure of a patient's entire record is justified, and that such disclosure does not require individual review, when requested for disease management purposes.

Response: The minimum necessary standard is not intended to impede essential treatment, payment, or health care operations activities of covered entities. Nor is the Rule intended to change the way covered entities handle their differences with respect to disclosures of protected health information. The Department recognizes that, in some cases, an individual's entire medical record may be necessary for payment or health care operations purposes, including disease management purposes. However, the Department does not believe that disclosure of a patient's entire medical record is always justified for such purposes. The Privacy Rule does not prohibit the request for, or release of, entire medical records in such circumstances, provided that the covered entity has documented the specific justification for the request or disclosure of the entire record.

Comment: A few commenters requested that the Department add to the regulatory text some of the statements included in the preamble to the proposed modifications. For example, commenters asked that the final Rule state that the minimum necessary standard is ''intended to be consistent with, and not override, professional judgement and standards.'' Similarly, others requested that the regulation specify that ''covered entities must implement policies and procedures based on their own assessment of what protected health information is reasonably necessary for a particular purpose, given the characteristics of their business and their workforce, and using their own professional judgment.''

Response: It is the Department's policy that the minimum necessary standard is intended to be consistent with, and not override, professional judgment and standards, and that covered entities must implement policies and procedures based on their own assessment of what protected health information is reasonably necessary for a particular purpose, given the characteristics of their business and their workforce. However, the Department does not believe a regulatory modification is necessary because the Department has made its policy clear not only in the preamble to the proposed modifications but also in previous guidance and in this preamble.

Comment: A commenter argued that the Department should exempt disclosures for any of the standard transactions as required by the Transactions Rule, when information is requested by a health plan or its business associate.

Response: The Department disagrees. The Privacy Rule already exempts from the minimum necessary standard data elements that are required or situationally required in any of the standard transactions (§ 164.502(b)(2)(v)). If, however, a standard transaction permits the use of optional data elements, the minimum necessary standard applies. For example, the standard transactions adopted for the outpatient pharmacy sector use optional data elements. The payer currently specifies which of the optional data elements are needed for payment of its particular pharmacy claims. The minimum necessary standard applies to the payer's request for such information. A pharmacist is permitted to rely on the payer's request for information, if reasonable to do so, as the minimum necessary for the intended disclosure.

Comment: A few commenters expressed concerns with respect to a covered entity's disclosures for research purposes. Specifically, one commenter was concerned that a covered entity will not accept documentation of an external IRB's waiver of authorization for purposes of reasonably relying on the request as the minimum necessary. It was suggested that the Department deem that a disclosure to a researcher based on appropriate documentation from an IRB or Privacy Board meets the minimum necessary standard.

Response: The Department understands commenters' concerns that covered entities may decline to

participate in research studies, but believes that the Rule already addresses this concern. The Privacy Rule explicitly permits a covered entity reasonably to rely on a researcher's documentation or the representations of an IRB or Privacy Board pursuant to § 164.512(i) that the information requested is the minimum necessary for the research purpose. This is true regardless of whether the documentation is obtained from an external IRB or Privacy Board or one that is associated with the covered entity. The preamble to the March 2002 NPRM further reinforced this policy by stating that reasonable reliance on an IRB's documentation of approval of the waiver criteria and a description of the data needed for the research as required by § 164.512(i) would satisfy a covered entity's obligations with respect to limiting the disclosure to the minimum necessary. The Department reiterates this policy here and believes that this should give covered entities sufficient confidence in accepting IRB waivers of authorization.

Comment: A number of commenters requested that the Department limit the amount of information that pharmacy benefits managers (PBM) may demand from pharmacies as part of their claims payment activities.

Response: The health plan, as a covered entity, is obligated to instruct the PBM, as its business associate acting through the business associate contract, to request only the minimum amount of information necessary to pay a claim. The pharmacist may rely on this determination if reasonable to do so, and then does not need to engage in a separate minimum necessary assessment. If a pharmacist does not agree that the amount of information requested is reasonably necessary for the PBM to fulfill its obligations, it is up to the pharmacist and PBM to negotiate a resolution of the dispute as to the amount of information needed by the PBM to carry out its obligations and that the pharmacist is willing to provide, recognizing that the PBM is not required to pay claims if it has not received the information it believes is necessary to process the claim in accordance with its procedures, including fraud prevention procedures.

The standard for electronic pharmacy claims, adopted by the Secretary in the Transactions Rule, includes optional data elements and relies on each payer to specify the data elements required for payment of its claims. Understandably, the majority of health plans require some patient identification elements in order to adjudicate claims. As the National Council for Prescription Drug Programs (NCPDP) moves from optional to required and situational data elements, the question of whether the specific element of ''patient name'' should be required or situational will be debated by the NCPDP, by the Designated Standards Maintenance Organizations, by the National Committee on Vital and Health Statistics, and ultimately will be decided in rulemaking by the Secretary.

Comment: One commenter requested that the minimum necessary standard be made an administrative requirement rather than a standard for uses and disclosures, to ease liability concerns with implementing the standard. The commenter stated that this change would mean that covered entities would be required to implement reasonable minimum necessary policies and procedures and would be liable if: (1) They fail to implement minimum necessary policies and procedures; (2) their policies and procedures are not reasonable; or (3) they fail to enforce their policies and procedures. The commenter further explained that health plans would be liable if their policies and procedures for requesting health information were unreasonable, but the burden of liability for the request shifts largely to the entity best suited to determine whether the amount of information requested is the minimum necessary.

Response: The Privacy Rule already requires covered entities to implement reasonable minimum necessary policies and procedures and to limit any use, disclosure, or request for protected health information in a manner consistent with its policies and procedures. The minimum necessary standard is an appropriate standard for uses and disclosures, and is not merely an administrative requirement. The Privacy Rule provides adequate flexibility to adopt minimum necessary policies and procedures that are workable for the covered entity, thereby minimizing a covered entity's liability concerns.

Comment: A number of commenters expressed concerns about application of the minimum necessary standard to disclosures for workers' compensation purposes. Commenters argued that the standard will prevent workers' compensation insurers and State administrators, as well as employers, from obtaining the information needed to pay injured workers the benefits guaranteed under the State workers' compensation system. They also argued that the minimum necessary standard could lead to fraudulent claims and unnecessary legal action in order to obtain information needed for workers' compensation purposes.

Response: The Privacy Rule is not intended to disrupt existing workers' compensation systems as established by State law. In particular, the Rule is not intended to impede the flow of health information that is needed by employers, workers' compensation carriers, or State officials in order to process or adjudicate claims and/or coordinate care under the workers' compensation system. To this end, the Privacy Rule at § 164.512(l) explicitly permits a covered entity to disclose protected health information as authorized by, and to the extent necessary to comply with, workers' compensation or other similar programs established by law that provide benefits for work-related injuries or illnesses without regard to fault. The minimum necessary standard permits covered entities to disclose any protected health information under § 164.512(l) that is reasonably necessary for workers' compensation purposes and is intended to operate so as to permit information to be shared for such purposes to the full extent permitted by State or other law.

Additionally, where a State or other law requires a disclosure of protected health information for workers' compensation purposes, such disclosure is permitted under § 164.512(a). A covered entity also is permitted to disclose protected health information to a workers' compensation insurer where the insurer has obtained the individual's authorization pursuant to § 164.508 for the release of such information. The minimum necessary provisions do not apply to disclosures required by law or made pursuant to authorizations. See § 164.502(b), as modified herein.

Further, the Department notes that a covered entity is permitted to disclose information to any person or entity as necessary to obtain payment for health care services. The minimum necessary provisions apply to such disclosures but permit the covered entity to disclose the amount and types of information that are necessary to obtain payment.

The Department also notes that because the disclosures described above are permitted by the Privacy Rule, there is no potential for conflict with State workers' compensation laws, and, thus, no possibility of preemption of such laws by the Privacy Rule.

The Department's review of certain States workers' compensation laws demonstrates that many of these laws address the issue of the scope of information that is available to carriers and employers. The Privacy Rule's minimum necessary standard will not create an obstacle to the type and

amount of information that currently is provided to employers, workers' compensation carriers, and State administrative agencies under these State laws. In many cases, the minimum necessary standard will not apply to disclosures made pursuant to such laws. In other cases, the minimum necessary standard applies, but permits disclosures to the full extent authorized by the workers' compensation laws. For example, Texas workers' compensation law requires a health care provider, upon the request of the injured employee or insurance carrier, to furnish records relating to the treatment or hospitalization for which compensation is being sought. Since such disclosure is required by law, it also is permissible under the Privacy Rule at § 164.512(a) and exempt from the minimum necessary standard. The Texas law further provides that a health care provider is permitted to disclose to the insurance carrier records relating to the diagnosis or treatment of the injured employee without the authorization of the injured employee to determine the amount of payment or the entitlement to payment. Since the disclosure only is permitted and not required by Texas law, the provisions at § 164.512(l) would govern to permit such disclosure. In this case, the minimum necessary standard would apply to the disclosure but would allow for information to be disclosed as authorized by the statute, that is, as necessary to ''determine the amount of payment or the entitlement to payment.''

As another example, under Louisiana workers' compensation law, a health care provider who has treated an employee related to a workers' compensation claim is required to release any requested medical information and records relative to the employee's injury to the employer or the workers' compensation insurer. Again, since such disclosure is required by law, it is permissible under the Privacy Rule at § 164.512(a) and exempt from the minimum necessary standard. The Louisiana law further provides that any information relative to any other treatment or condition shall be available to the employer or workers' compensation insurer through a written release by the claimant. Such disclosure also would be permissible and exempt from the minimum necessary standard under the Privacy Rule if the individual's written authorization is obtained consistent with the requirements of § 164.508.

The Department understands concerns about the potential chilling effect of the Privacy Rule on the workers' compensation system. Therefore, as the Privacy Rule is implemented, the Department will actively monitor the effects of the Rule on this industry to assure that the Privacy Rule does not have any unintended negative effects that disturb the existing workers' compensation systems. If the Department finds that, despite the above clarification of intent, the Privacy Rule is being misused and misapplied to interfere with the smooth operation of the workers' compensation systems, it will consider proposing modifications to the Rule to clarify the application of the minimum necessary standard to disclosures for workers' compensation purposes.

Comment: Another commenter urged the Department to clarify that a covered entity can reasonably rely on a determination made by a financial institution or credit card payment system regarding the minimum necessary information needed by that financial institution or payment system to complete a contemplated payment transaction.

Response: Except to the extent information is required or situationally required for a standard payment transaction (*see* 45 CFR 162.1601, 162.1602), the minimum necessary standard applies to a covered entity's disclosure of protected health information to a financial institution in order to process a payment transaction. With limited exceptions, the Privacy Rule does not allow a covered entity to substitute the judgment of a private, third party for its own assessment of the minimum necessary information for a disclosure. Under the exceptions in § 164.514(d)(3)(iii), a covered entity is permitted reasonably to rely on the request of another covered entity because, in this case, the requesting covered entity is itself subject to the minimum necessary standard and, therefore, required to limit its request to only that information that is reasonably necessary for the purpose. Thus, the Department does not agree that a covered entity should generally be permitted reasonably to rely on the request of a financial institution as the minimum necessary. However, the Department notes that where, for example, a financial institution is acting as a business associate of a covered entity, the disclosing covered entity may reasonably rely on a request from such financial institution, because in this situation, both the requesting and disclosing entity are subject to the minimum necessary standard.

Comment: A number of commenters continued to request additional guidance with respect to implementing this discretionary standard. Many expressed support for the statement in the NPRM that HHS intends to issue further guidance to clarify issues causing confusion and concern in industry, as well as provide additional technical assistance materials to help covered entities implement the provisions.

Response: The Department is aware of the need for additional guidance in this area and intends to provide technical assistance and further clarifications as necessary to address these concerns and questions.

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

December 2000 Privacy Rule. The Privacy Rule is intended to assure that parents have appropriate access to health information about their children. By creating new Federal protections and individual rights with respect to individually identifiable health information, parents will generally have new rights with respect to the health information about their minor children. In addition, the Department intended that the disclosure of health information about a minor child to a parent should be governed by State or other applicable law.

Under the Privacy Rule, parents are granted new rights 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 under State or other applicable laws of certain minors to obtain specified health care without parental consent. 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 the 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 December 2000 Privacy Rule. (*See* § 164.502(g)(3)(i) and (ii), redesignated as § 164.502(g)(3)(i)(A) and (B)).

The December 2000 Privacy Rule also allows the minor to exercise control of

[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.*

protected health information when the parent has agreed to the minor obtaining confidential treatment (*see* § 164.502(g)(3)(iii), redesignated as § 164.502(g)(3)(i)(C) in this final Rule), 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 may disclose health information about a minor to a parent in the most critical situations, 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 adopted in December 2000 also states that disclosure of health information about a minor to a parent is permitted if State law authorizes 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), redesignated as § 164.502(g)(3)(i)(A), 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 few exceptions listed above.

March 2002 NPRM. After reassessing the parents and minors provisions in the Privacy Rule, the Department identified two areas in which there were unintended consequences of the Rule. First, the language regarding deference to State law, which authorizes or prohibits disclosure of health information about a minor to a parent, fails to assure that State or other law governs when the law grants a provider discretion in certain circumstances to disclose protected health information to a parent. Second, the Privacy Rule may have prohibited parental access in certain situations in which State or other law may have permitted such access.

The Department proposed changes to these standards where they did not operate as intended and did not adequately defer to State or other applicable law with respect to parents and minors. 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 proposed 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.

Second, the Department proposed 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 his or her minor child under § 164.524, in the rare circumstance in which the parent is technically not the personal representative of his or her minor child under the Privacy Rule. This policy would apply particularly where State or other law is silent or unclear.

Overview of Public Comments. The following discussion provides an overview of the public comment received on this proposal. Additional comments received on this issue are discussed below in the section entitled, ''Response to Other Public Comments.''

The Department received a number of comments on the proposed changes to the parents and minors provisions of the Privacy Rule. Many commenters, particularly health care providers involved in provision of health care to minors, requested that the Department return to the approach under the Privacy Rule published in December 2000, because they believed that the proposed approach would discourage minors from seeking necessary health care. At a minimum, these commenters suggested that the Department clarify that discretion to grant a parent access under the proposal is limited to the covered health care provider that is providing treatment to the minor.

Supporters of the proposal asserted that the Department was moving in the right direction, but many also advocated for more parental rights. They asserted that parents have protected rights to act for their children and that the Privacy Rule interferes with these rights.

There were also some commenters that were confused by the new proposal and others that requested a Federal standard that would preempt all State laws.

Final Modifications. The Department will continue to defer to State or other applicable law and to remain neutral to the extent possible. However, the Department is adopting changes to the standards in the December 2000 Privacy Rule, where they do not operate as intended and are inconsistent with the Department's underlying goals. These modifications are similar in approach to the NPRM and the rationale for these changes remains the same as was stated in the NPRM. However, the Department makes some changes from the language that was proposed, in order to simplify the provisions and clarify the Department's intent.

There are three goals with respect to the parents and minors provisions in the Privacy Rule. First, the Department wants to assure that parents have appropriate access to the health information about their minor children to make important health care decisions about them, while also making sure that the Privacy Rule does not interfere with a minor's ability to consent to and obtain health care under 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 with the health care practices of such providers with respect to adolescent health care.

In order to honor these differing goals, the Department has and continues to take the approach of deferring to State or other applicable law and professional practice with respect to parents and minors. Where State and other applicable law is silent or unclear, the Department has attempted to create standards, implementation specifications, and requirements that are consistent with such laws and that permit States the discretion to continue to define the rights of parents and minors with respect to health information without interference from the Federal Privacy Rule.

The Department adopts two changes to the provisions regarding parents and minors in order to address unintended consequences from the December 2000 Privacy Rule and to defer to State and other law. The first change is about disclosure of protected health information to a parent and the second is about access to the health information by the parent. Disclosure is about a covered entity providing individually identifiable information to persons outside the entity, either the individual or a third party. Access is a particular type of disclosure that is the right of an individual (directly or through a personal representative) to review or

obtain a copy of his or her health information under § 164.524. This modification treats both activities similarly by deferring to State or other applicable law.

The first change, regarding disclosure of protected health information to a parent, is the same as the change proposed in the NPRM. 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 language in the definition of ''more stringent'' (*see* § 160.202) that addresses the disclosure of protected health information about a minor to a parent has been moved to the standards regarding parents and minors (*see* § 164.502(g)(3)). The addition of paragraphs (g)(3)(ii)(A) and (B) of § 164.502, clarify that State and other applicable law governs when such law explicitly requires, permits, or prohibits disclosure of protected health information to a parent.

In connection with moving the language, the language is changed from the December 2000 Privacy Rule in order to adapt it to the new section. Section 164.502(g)(3)(ii)(A) 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 permits or requires such disclosure. By adopting this provision, the Department makes clear that nothing in the regulation prohibits disclosure of health information to a parent if, and to the extent that, State or other law permits or requires such disclosure. The Privacy Rule defers to such State or other law and permits covered entities to act in accordance to such law. Section 164.502(g)(3)(ii)(B) states 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 prohibits such disclosure. Again, regardless of how the Privacy Rule would operate in the absence of explicit State or other law, if such law prohibits the disclosure of protected health information about a minor to a parent, so does the Privacy Rule. The revision also clarifies that deference to State or other applicable law includes deference to established case law as well as explicit provisions in statutes or regulations that permit, require, or prohibit particular disclosures.

The second change, regarding access to protected health information, also reflects the same policy as proposed in the NPRM. There are two provisions that refer to access, in order to clarify the Department's intent in this area. The first is where there is an explicit State or other law regarding parental access, and the second is where State or other law is silent or unclear, which is often the case with access.

Like the provisions regarding disclosure of protected health information to a parent, the final Rule defers to State or other applicable law regarding a parent's access to health information about a minor. The change assures that State or other applicable law governs when the law explicitly requires, permits, or prohibits access to protected health information about a minor to a parent. This includes deference to established case law as well as an explicit provision in a statute or regulation. This issue is addressed in paragraphs (g)(3)(ii)(A) and (B) of § 164.502 with the disclosure provisions discussed above.

In addition to the provision regarding explicit State access laws, the Department recognizes that the Privacy Rule creates a right of access that previously did not exist in most States. Most States do not have explicit laws in this area. In order to address the limited number of cases in which the parent is not the personal representative of the minor because one of the exceptions in the parents and minors provisions are met (*see* § 164.502(g)(3)(i)(A), (B), or (C)), the Department adds a provision, § 164.502(g)(3)(ii)(C), similar to a provision proposed in the NPRM, that addresses those situations in which State and other law about parental access is not explicit. Under this provision, a covered entity may provide or deny access to a parent provided that such discretion is permitted by State or other law. This new paragraph would assure that the Privacy Rule would not prevent a covered entity from providing access to a parent if the covered entity would have been able to provide this access under State or other applicable law. The new paragraph would also prohibit access by a parent if providing such access would violate State or other applicable law.

It is important to note that this provision regarding access to health information about a minor in cases in which State and other laws are silent or unclear will not apply in the majority of cases because, typically, the parent will be the personal representative of his or her minor child and will have a right of access to the medical records of his or her minor children under the Privacy Rule. This provision only applies in cases in which the parent is not the personal representative under the Privacy Rule.

In response to comments by health care providers, the final modifications also clarify that, the discretion to provide or deny access to a parent under § 164.502(g)(3)(ii)(C) only may be exercised by a licensed health care professional, in the exercise of professional judgment. This is consistent with the policy described in the preamble to the NPRM, is similar to the approach in the access provisions in § 164.524(a)(3), and furthers the Department's interest in balancing the goals of providing appropriate information to parents and of assuring that minors obtain appropriate access to health care. This decision should be made by a health care professional, who is accustomed to exercising professional judgment. A health plan may also exercise such discretion if the decision is made by a licensed health care provider.

The Department takes no position on the ability of a minor to consent to treatment and no position on how State or other law affects privacy between the minor and parent. Where State or other law is unclear, covered entities should continue to conduct the same analysis of such law as they do now to determine if access is permissible or not. Because the Privacy Rule defers to State and other law in the area of parents and minors, the Department assumes that the current practices of health care providers with respect to access by parents and confidentiality of minor's records are consistent with State and other applicable law, and, therefore, can continue under the Privacy Rule.

Parental access under this section would continue to be subject to any limitations on activities of a personal representative in § 164.502(g)(5) and § 164.524(a)(2) and (3). In cases in which the parent is not the personal representative of the minor and State or other law does not require parental access, this provision does not provide a parent a right to demand access and does not require a covered entity to provide access to a parent. Furthermore, nothing in these modifications shall affect whether or not a minor would have a right to access his or her records. That is, a covered entity's exercise of discretion to not grant a parent access does not affect the right of access the minor may have under the Privacy Rule. A covered entity may deny a parent access in accordance with State or other law and may be required to provide access to the minor under the Privacy Rule.

These changes also do not affect the general provisions, explained in the section ''December 2000 Privacy Rule'' above, regarding parents as personal representatives of their minor children or the exceptions to this general rule, where parents would not be the

personal representatives of their minor children.

These changes adopted in this Rule provide States with the option of clarifying the interaction between their laws regarding consent to health care and the ability of parents to have access to the health information about the care received by their minor children in accordance with such laws. As such, this change should more accurately reflect current State and other laws and modifications to such laws.

Response to Other Public Comments

Comment: Some commenters urged the Department to retain the approach to parents and minors that was adopted in December 2000. They claimed that the NPRM approach would seriously undermine minors' willingness to seek necessary medical care. Other commenters advocated full parental access to health information about their minor children, claiming that the Privacy Rule interferes with parents' rights.

Response: We believe the approach adopted in the final Rule strikes the right balance between these concerns. It defers to State law or other applicable law and preserves the status quo to the greatest extent possible.

Comment: Health care providers generally opposed the changes to the parents and minors provisions claiming that they would eliminate protection of a minor's privacy, and therefore, would decrease the willingness of adolescents to obtain necessary health care for sensitive types of health care services. They also argued that the NPRM approach is inconsistent with State laws that give minors the right to consent to certain health care because the purpose of these laws is to provide minors with confidential health care.

Response: Issues related to parents' and minors' rights with respect to health care are best left for the States to decide. The standards regarding parents and minors are designed to defer to State law in this area. While we believe that there is a correlation between State laws that grant minors the authority to consent to treatment and confidentiality of the information related to such treatment, our research has not established that these laws bar parental access to such health information under all circumstances. Therefore, to act in a manner consistent with State law, the approach adopted in this Final Rule is more flexible than the standards adopted in December 2000, in order to assure that the Privacy Rule does not preclude a provider from granting access to a parent if this is permissible under State law. However, this new standard would not permit activity that would be impermissible under State law.

Some State or other laws may state clearly that a covered entity must provide a parent access to the medical records of his or her minor child, even when the minor consents to the treatment without the parent. In this case, the covered entity must provide a parent access, subject to the access limitations in the Privacy Rule at § 164.524(a)(2) and (3). Other laws may state clearly that a covered entity must not provide a parent access to their minor child's medical records when the minor consents to the treatment without the parent. In this case, the covered entity would be precluded from granting access to the parent. If the State or other law clearly provides a covered entity with discretion to grant a parent access, then the covered entity may exercise such discretion, to the extent permitted under such other law.

If State law is silent or unclear on its face, then a covered entity would have to go through the same analysis as it would today to determine if such law permitted, required, or prohibited providing a parent with access to a minor's records. That analysis may involve review of case law, attorney general opinions, legislative history, etc. If such analysis showed that the State would permit an entity to provide a parent access to health information about a minor child, and under the Privacy Rule, the parent would not be the personal representative of the minor because of one of the limited exceptions in § 164.502(g)(3)(i), then the covered entity may exercise such discretion, based on the professional judgment of a licensed health care provider, to choose whether or not to provide the parent access to the medical records of his or her minor child. If, as the commenters suggest, a State consent law were interpreted to prohibit such access, then such access is prohibited under the Privacy Rule as well.

Comment: One commenter asserted that the Privacy Rule inappropriately erects barriers between parents and children. Specifically, the commenter stated that § 164.502(g)(5) delegates to private entities government power to decide whether a child may be subjected to abuse or could be endangered. The commenter also stated that the access provisions in § 164.502(g)(3) would erect barriers where State law is silent or unclear.

Response: The Department does not agree that the Privacy Rule erects barriers between a parent and a minor child because the relevant standards are intended to defer to State law. Health care providers have responsibilities under other laws and professional standards to report child abuse to the appropriate authorities and to use professional discretion to protect the child's welfare in abuse situations. Similarly the Privacy Rule permits (but does not require) the provider to use professional discretion to act to protect a child she believes is being abused. If the Privacy Rule were to mandate that a provider grant a parent access to a medical record in abuse situations, as the commenter suggests, this would be a change from current law. In addition, the Privacy Rule does not allow a denial of parental access to medical records if State or other law would require such access.

Comment: Commenters continue to raise preemption issues. A few commenters called for preemption of all State law in this area. Others stated that there should be one standard, not 50 standards, controlling disclosure of protected health information about a minor to a parent and that the NPRM approach would burden regional and national health care providers. Others urged preemption of State laws that are less protective of a minor's privacy, consistent with the general preemption provisions.

Response: The Department does not want to interfere with a State's role in determining the appropriate rights of parents and their minor children. The claim that the Privacy Rule introduces 50 standards is inaccurate. These State standards exist today and are not created by the Privacy Rule. Our approach has been, and continues to be, to defer to State and other applicable law in this area.

Comment: One commenter requested the Privacy Rule state that good faith compliance with the Privacy Rule is an affirmative defense to enforcement of contrary laws ultimately determined to be more stringent than the Rule, or that it provide specific guidance on which State laws conflict with or are more stringent than the Privacy Rule.

Response: The Privacy Rule cannot dictate how States enforce their own privacy laws. Furthermore, guidance on whether or not a State law is preempted would not be binding on a State interpreting its own law.

Comment: Some commenters remain concerned that a parent will not get information about a child who receives care in an emergency without the consent of the parent and that the provisions in § 164.510(b) are not sufficient.

Response: As we have stated in previous guidance, a provider generally can discuss all the health information

about a minor child with his parent, because the parent usually will be the personal representative of the child. This is true, under the Privacy Rule, even if the parent did not provide consent to the treatment because of the emergency nature of the health care. A parent may be unable to obtain such information in limited circumstances, such as when the minor provided consent for the treatment in accordance with State law or the treating physician suspects abuse or neglect or reasonably believes that releasing the information to the parent will endanger the child.

Comment: A couple of commenters were concerned that the provisions regarding confidential communications conflict with the Fair Debt Collection Practices Act (FDCPA), which allows collection agencies to contact the party responsible for payment of the debt, be it the spouse or parent (of a minor) of the individual that incurred the debt, and share information that supports the incurrence and amount of the debt. They feared that the Privacy Rule would no longer allow collection agencies to continue this practice.

Response: Our analysis of the relevant provisions of the Privacy Rule and the FDCPA does not indicate any conflicts between the two laws. An entity that is subject to the FDCPA and the Privacy Rule (or that must act consistent with the Privacy Rule as a business associate of the covered entity) should be able to comply with both laws, because the FDCPA permits an entity to exercise discretion to disclose information about one individual to another.

The FDCPA allows debt collectors to communicate with the debtor's spouse or parent if the debtor is a minor. The provisions of the FDCPA are permissive rather than required.

Generally, the Privacy Rule permits covered entities to use the services of debt collectors as the use of such services to obtain payment for the provision of health care comes within the definition of ''payment.'' The Privacy Rule generally does not identify to whom information can be disclosed when a covered entity is engaged in its own payment activities. Therefore, if a covered entity or a debt collector, as a business associate of a covered entity, needs to disclose protected health information to a spouse or a parent, the Privacy Rule generally would not prevent such disclosure. In these cases where the Privacy Rule would permit disclosure to a parent or spouse, there should be no concern with the interaction with the FDCPA.

However, there are some circumstances in which the Privacy Rule may prohibit a disclosure to a parent or a spouse for payment purposes. For example, under § 164.522(a), an individual has the right to request restrictions to the disclosure of health information for payment. A provider or health plan may choose whether or not to agree to the request. If the covered entity agreed to a restriction, the covered entity would be bound by that restriction and would not be permitted to disclose the individual's health information in violation of that agreement. Also, § 164.522(b) generally requires covered entities to accommodate reasonable requests by individuals to receive communications of protected health information by alternative means or at alternative locations. However, the covered entity may condition the accommodation on the individual providing information on how payment will be handled. In both of these cases, the covered entity has means for permitting disclosures as permitted by the FDCPA. Therefore, these provisions of the Privacy Rule need not limit options available under the FDCPA. However, if the agreed-to restrictions or accommodation for confidential communications prohibit disclosure to a parent or spouse of an individual, the covered entity, and the debt collector as a business associate of the covered entity, would be prohibited from disclosing such information under the Privacy Rule. In such case, because the FDCPA would provide discretion to make a disclosure, but the Privacy Rule would prohibit the disclosure, a covered entity or the debt collector as a business associate of a covered entity would have to exercise discretion granted under the FDCPA in a way that complies with the Privacy Rule. This means not making the disclosure.

C. Section 164.504—Uses and Disclosures: Organizational Requirements

1. Hybrid Entities

December 2000 Privacy Rule. The Privacy Rule, as published in December 2000, defined covered entities that primarily engage in activities that are not ''covered functions,'' that is, functions that relate to the entity's operation as a health plan, health care provider, or health care clearinghouse, as hybrid entities. *See* 45 CFR 164.504(a). Examples of hybrid entities were: (1) corporations that are not in the health care industry, but that operate on-site health clinics that conduct the HIPAA standard transactions electronically; and (2) insurance carriers that have multiple lines of business that include both health insurance and other insurance lines, such as general liability or property and casualty insurance.

Under the December 2000 Privacy Rule, a hybrid entity was required to define and designate those parts of the entity that engage in covered functions as one or more health care component(s). A hybrid entity also was required to include in the health care component(s) any other components of the entity that support the covered functions in the same way such support may be provided by a business associate (e.g., an auditing component). The health care component was to include such ''business associate'' functions for two reasons: (1) It is impracticable for the entity to contract with itself; and (2) having to obtain an authorization for disclosures to such support components would limit the ability of the hybrid entity to engage in necessary health care operations functions. In order to limit the burden on hybrid entities, most of the requirements of the Privacy Rule only applied to the health care component(s) of the entity and not to the parts of the entity that do not engage in covered functions.

The hybrid entity was required to create adequate separation, in the form of firewalls, 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 was a disclosure under the Privacy Rule and was allowed only to the same extent such a disclosure was permitted to a separate entity.

In the preamble to the December 2000 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 further explained that it 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 a covered function, then the whole entity would have been a covered entity and the hybrid entity provisions would not have applied. However, if the covered entity primarily conducted non-health activities, it would have qualified as a hybrid entity and would have been required to comply with the Privacy Rule with respect to its health care component(s). *See* 65 FR 82502.

March 2002 NPRM. Since the publication of the final Rule, concerns were raised that the policy guidance in the preamble was insufficient so long as the Privacy Rule itself limited the hybrid entity provisions to entities that primarily conducted non-health related activities. In particular, concerns were

raised about whether entities, which have the health plan line of business as the primary business and an excepted benefits line, such as workers' compensation insurance, as a small portion of the business, qualified as hybrid entities. There were also concerns about how ''primary'' was to be defined, if it was not a mathematical calculation, and how an 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 proposed to delete the term ''primary'' from the definition of ''hybrid entity'' in § 164.504(a) and permit any covered entity that is a single legal entity and that performs both covered and non-covered functions to choose whether or not to be a hybrid entity for purposes of the Privacy Rule. Under the proposal, any covered entity could be a hybrid entity regardless of whether the non-covered functions represent the entity's primary functions, a substantial function, or even a small portion of the entity's activities. In order to be a hybrid entity under the proposal, a covered entity would have to designate its health care component(s). If the covered entity did not designate any health care component(s), the entire entity would be a covered entity and, therefore, subject to the Privacy Rule. Since the entire entity would be the covered entity, § 164.504(c)(2) requiring firewalls between covered and non-covered portions of hybrid entities would not apply.

The Department explained in the preamble to the proposal that there are advantages and disadvantages to being a hybrid entity. Whether or not the advantages outweigh the disadvantages would be a decision for each covered entity that qualified as a hybrid entity, taking into account factors such as how the entity was organized and the proportion of the entity that must be included in the health care component.

The Department also proposed 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 proposed § 164.504(c)(3)(iii). The Department proposed to move the specific language regarding which components make up a health care component to the implementation specification that addresses designation of health care components at § 164.504(c)(3)(iii). At § 164.504(c)(3)(iii), the Department proposed that a health care component could 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. In addition, the Department proposed to make clear at § 164.504(c)(3)(iii) that a hybrid entity must designate as a health care component(s) any component that would meet the definition of ''covered entity'' if it were a separate legal entity.

There was some ambiguity in the December 2000 Privacy Rule as to whether a health care provider that does not conduct electronic transactions for which the Secretary has adopted standards (*i.e.,* a non-covered health care provider) and which is part of a larger covered entity was required to be included in the health care component. To clarify this issue, the proposal also would allow a hybrid entity the discretion to include in its health care component a non-covered health care provider component. Including a non-covered health care provider in the health care component would subject the non-covered provider to the Privacy Rule. Accordingly, the Department proposed a conforming change in § 164.504(c)(1)(ii) to make 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.

The proposal also would permit a hybrid entity to designate otherwise non-covered portions of its operations that provide services to the covered functions, such as parts of the legal or accounting divisions of the entity, as part of the health care component, so that protected health information could be shared with such functions of the entity without business associate agreements or individual authorizations. The proposal would not require that the covered entity designate entire divisions as in or out of the covered component. Rather, it would permit the covered entity to designate functions within such divisions, such as the functions of the accounting division that support health insurance activities, without including those functions that support life insurance activities. The Department proposed to delete as unnecessary and redundant 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.

Overview of Public Comments. The following discussion provides an overview of the public comment received on this proposal. Additional comments received on this issue are discussed below in the section entitled, ''Response to Other Public Comments.''

The Department received relatively few comments on its proposal regarding hybrid entities. A number of comments supported the proposal, appreciative of the added flexibility it would afford covered entities in their compliance efforts. For example, some drug stores stated that the proposal would provide them with the flexibility to designate health care components, whereas under the December 2000 Rule, these entities would have been required to subject their entire business, including the ''front end'' of the store which is not associated with dispensing prescription drugs, to the Privacy Rule's requirements.

Some health plans and other insurers also expressed strong support for the proposal. These comments, however, seemed to be based on a misinterpretation of the uses and disclosures the proposal actually would permit. These commenters appear to assume that the proposal would allow information to flow freely between non-covered and covered functions in the same entity, if that entity chose not to be a hybrid entity. For example, commenters explained that they interpreted the proposal to mean that a multi-line insurer which does not elect hybrid entity status would be permitted to share protected health information between its covered lines and its otherwise non-covered lines. It was stated that such latitude would greatly enhance multi-line insurers' ability to detect and prevent fraudulent activities and eliminate barriers to sharing claims information between covered and non-covered lines of insurance where necessary to process a claim.

Some commenters opposed the Department's hybrid entity proposal, stating that the proposal would reduce the protections afforded under the Privacy Rule and would be subject to abuse. Commenters expressed concerns that the proposal would allow a covered entity with only a small health care component to avoid the extra protections of creating firewalls between the health care component and the rest of the organization. Moreover, one of the commenters stated that the proposal could allow a covered entity that is primarily performing health care functions to circumvent the requirements of the Rule for a large part of its operations by designating itself a hybrid and excluding from the health

care component a non-covered health care provider function, such as a free nurse advice line that does not bill electronically. In addition, it was stated that the ambiguous language in the proposal could potentially be construed as allowing a hybrid entity to designate only the business associate-like functions as the health care component, and exclude covered functions. The commenter urged the Department to clarify that a hybrid entity must, at a minimum, designate a component that performs covered functions as a health care component, and that a health care provider cannot avoid having its treatment component considered a health care component by relying on a billing department to conduct its standard electronic transactions. These commenters urged the Department to retain the existing policy by requiring those organizations whose primary functions are not health care to be hybrid entities and to institute firewall protections between their health care and other components.

Final Modifications. After consideration of the comments, the Department adopts in the final Rule the proposed approach to provide covered entities that otherwise qualify the discretion to decide whether to be a hybrid entity. To do so, the Department eliminates the term ''primary'' from the definition of ''hybrid entity'' at § 164.504(a). Any covered entity that otherwise qualifies (*i.e.,* is a single legal entity that performs both covered and non-covered functions) and that designates health care component(s) in accordance with § 164.504(c)(3)(iii) is a hybrid entity. A hybrid entity is required to create adequate separation, in the form of firewalls, 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 continues to be a disclosure under the Privacy Rule, and, thus, allowed only to the same extent such a disclosure is permitted to a separate entity.

Most of the requirements of the Privacy Rule continue to apply only to the health care component(s) of a hybrid entity. Covered entities that choose not to designate health care component(s) are subject to the Privacy Rule in their entirety.

The final Rule regarding hybrid entities is intended to provide a covered entity with the flexibility to apply the Privacy Rule as best suited to the structure of its organization, while maintaining privacy protections for protected health information within the organization. In addition, the policy in the final Rule simplifies the Privacy Rule and makes moot any questions about what ''primary'' means for purposes of determining whether an entity is a hybrid entity.

The final Rule adopts the proposal's simplified definition of ''health care component,'' which makes clear that a health care component is what the covered entity designates as the health care component. The Department makes a conforming change in § 164.504(c)(2)(ii) to reflect the changes to the definition of ''health care component.'' The final Rule at § 164.504(c)(3)(iii) requires a health care component to include a component that would meet the definition of a ''covered entity'' if it were a separate legal entity. The Department also modifies the language of the final Rule at § 164.504(c)(3)(iii) to clarify that only a component that performs covered functions, and a component to the extent that it performs covered functions or activities that would make such component a business associate of a component that performs covered functions if the two components were separate legal entities, may be included in the health care component. ''Covered functions'' are defined at § 164.501 as ''those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.''

As in the proposal, the Department provides a hybrid entity with some discretion as to what functions may be included in the health care component in two ways. First, the final Rule clarifies that a hybrid entity may include in its health care component a non-covered health care provider component. Accordingly, the Department adopts the proposed conforming change to § 164.504(c)(1)(ii) to make clear that a reference to a ''covered health care provider'' in the Privacy Rule may include the functions of a health care provider who does not engage in electronic transactions for which the Secretary has adopted standards, if the covered entity chooses to include such functions in the health care component. A hybrid entity that chooses to include a non-covered health care provider in its health care component is 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.

Second, the final Rule retains the proposed policy to provide hybrid entities with discretion as to whether or not to include business associate-like divisions within the health care component. It is not a violation of the Privacy Rule to exclude such divisions from the health care component. However, a disclosure of protected health information from the health care component to such other division that is not part of the health care component is the same as a disclosure outside the covered entity. Because an entity cannot have a business associate contract with itself, such a disclosure likely will require individual authorization.

The Department clarifies, in response to comments, that a health care provider cannot avoid being a covered entity and, therefore, part of a health care component of a hybrid entity just by relying on a billing department to conduct standard transactions on its behalf. A health care provider is a covered entity if standard transactions are conducted on his behalf, regardless of whether the provider or a business associate (or billing department within a hybrid entity) actually conducts the transactions. In such a situation, however, designating relevant parts of the business associate division as part of the health care component would facilitate the conduct of health care operations and payment.

Also in response to comments, the Department clarifies that even if a covered entity does not choose to be a hybrid entity, and therefore is not required to erect firewalls around its health care functions, the entity still only is allowed to use protected health information as permitted by the Privacy Rule, for example, for treatment, payment, and health care operations. Additionally, the covered entity is still subject to minimum necessary restrictions under §§ 164.502 and 164.514(d), and, thus, must have policies and procedures that describe who within the entity may have access to the protected health information. Under these provisions, workforce members may be permitted access to protected health information only as necessary to carry out their duties with respect to the entity's covered functions. For example, the health insurance line of a multi-line insurer is not permitted to share protected health information with the life insurance line for purposes of determining eligibility for life insurance benefits or any other life insurance purposes absent an individual's written authorization. However, the health insurance line of a multi-line insurer may share protected health information with another line of business pursuant to § 164.512(a), if, for example, State law requires an insurer that receives a claim under one policy to share that information with other lines of insurance to determine if the event also may be payable under

another insurance policy. Furthermore, the health plan may share information with another line of business if necessary for the health plan's coordination of benefits activities, which would be a payment activity of the health plan.

Given the above restrictions on information flows within the covered entity, the Department disagrees with those commenters who raised concerns that the proposed policy would weaken the Rule by eliminating the formal requirement for ''firewalls.'' Even if a covered entity does not designate health care component(s) and, therefore, does not have to establish firewalls to separate its health care function(s) from the non-covered functions, the Privacy Rule continues to restrict how protected health information may be used and shared within the entity and who gets access to the information.

Further, the Department does not believe that allowing a covered entity to exclude a non-covered health care provider component from its health care component will be subject to abuse. Excluding health care functions from the health care component has significant implications under the Rule. Specifically, the Privacy Rule treats the sharing of protected health information from a health care component to a non-covered component as a disclosure, subject to the same restrictions as a disclosure between two legally separate entities. For example, if a covered entity decides to exclude from its health care component a non-covered provider, the health care component is then restricted from disclosing protected health information to that provider for any of the non-covered provider's health care operations, absent an individual's authorization. *See* § 164.506(c). If, however, the non-covered health care provider function is not excluded, it would be part of the health care component and that information could be used for its operations without the individual's authorization.

Response to Other Public Comments

Comment: A number of academic medical centers expressed concern that the Privacy Rule prevents them from organizing for compliance in a manner that reflects the integration of operations between the medical school and affiliated faculty practice plans and teaching hospitals. These commenters stated that neither the proposal nor the existing Rule would permit many academic medical centers to designate themselves as either a hybrid or affiliated entity, since the components of each must belong to a single legal entity or share common ownership or control. These commenters also explained that a typical medical school would not appear to qualify as an organized health care arrangement (OHCA) because it does not engage in any of the requisite joint activities, for example, quality assessment and improvement activities, on behalf of the covered entity. It was stated that it is essential that there not be impediments to the flow of information within an academic medical center. These commenters, therefore, urged that the Department add a definition of ''academic medical center'' to the Privacy Rule and modify the definition of ''common control'' to explicitly apply to the components of an academic medical center, so as to ensure that academic medical centers qualify as affiliated entities for purposes of the Rule.

Response: The Department does not believe that a modification to include a special rule for academic medical centers is warranted. The Privacy Rule's organizational requirements at § 164.504 for hybrid entities and affiliated entities, as well as the definition of ''organized health care arrangement'' in § 164.501, provide covered entities with much flexibility to apply the Rule's requirements as best suited to the structure of their businesses. However, in order to maintain privacy protections, the Privacy Rule places appropriate conditions on who may qualify for such organizational options, as well as how information may flow within such constructs. Additionally, if the commenter is suggesting that information should flow freely between the covered and non-covered functions within an academic medical center, the Department clarifies that the Privacy Rule restricts the sharing of protected health information between covered and non-covered functions, regardless of whether the information is shared within a single covered entity or a hybrid entity, or among affiliated covered entities or covered entities participating in an OHCA. Such uses and disclosures may only be made as permitted by the Rule.

Comment: A few commenters expressed concern with respect to governmental hybrid entities having to include business associate-like divisions within the health care component or else being required to obtain an individual's authorization for disclosures to such division. It was stated that this concept does not take into account the organizational structures of local governments and effectively forces such governmental hybrid entities to bring those components that perform business associate type functions into their covered component. Additionally, a commenter stated that this places an undue burden on local government by essentially requiring that functions, such as auditor/controller or county counsel, be treated as fully covered by the Privacy Rule in order to minimize otherwise considerable risk. Commenters, therefore, urged that the Department allow a health care component to enter into a memorandum of understanding (MOU) or other agreement with the business associate division within the hybrid entity. Alternatively, it was suggested that a governmental hybrid entity be permitted to include in its notice of privacy practices the possibility that information may be shared with other divisions within the same government entity for specific purposes.

Response: The Department clarifies that a covered entity which chooses to include its business associate division within the health care component may only do so to the extent such division performs activities on behalf of, or provides services to, the health care component. That same division's activities with respect to non-covered activities may not be included. To clarify this point, the Department modified the proposed language in § 164.504(c)(3)(iii) to provide that a health care component may only include a component to the extent that it performs covered functions or activities that would make such component a business associate of a component that performs covered functions if the two components were separate legal entities. For example, employees within an accounting division may be included within the health care component to the extent that they provide services to such component. However, where these same employees also provide services to non-covered components of the entity, their activities with respect to the health care component must be adequately separated from their other non-covered functions.

While the Department does not believe that a MOU between governmental divisions within a hybrid entity may be necessary given the above clarification, the Department notes that a governmental hybrid entity may elect to have its health care component enter into a MOU with its business associate division, provided that such agreement is legally binding and meets the relevant requirements of § 164.504(e)(3) and (e)(4). Such agreement would eliminate the need for the health care component to include the business associate division or for obtaining the

individual's authorization to disclose to such division.

Additionally, the Department encourages covered entities to develop a notice of privacy practices that is as specific as possible, which may include, for a government hybrid entity, a statement that information may be shared with other divisions within the government entity as permitted by the Rule. However, the notice of privacy practices is not an adequate substitute for, as appropriate, a memorandum of understanding; designation of business associate functions as part of a health care component; or alternatively, conditioning disclosures to such business associate functions on individuals' authorizations.

Comment: One commenter requested a clarification that a pharmacy-convenience store, where the pharmacy itself is a separate enclosure under supervision of a licensed pharmacist, is not a hybrid entity.

Response: The Department clarifies that a pharmacy-convenience store, if a single legal entity, is permitted, but not required, to be a hybrid entity and designate the pharmacy as the health care component. Alternatively, such an entity may choose to be a covered entity in its entirety. However, if the pharmacy and the convenience store are separate legal entities, the convenience store is not a covered entity simply by virtue of sharing retail space with the covered pharmacy.

Comment: Another commenter stated that the Rule implies that individual providers, once covered, are covered for all circumstances even if they are employed by more than one entity—one sending transactions electronically but not the other—or if the individual provider changes functions or employment and no longer electronically transmits standard transactions. This commenter asked that either the Rule permit an individual provider to be a hybrid entity (recognizing that there are times when an individual provider may be engaging in standard transactions, and other times when he is not), or that the definition of a ''covered entity'' should be modified so that individual providers are themselves classified as covered entities only when they are working as individuals.

Response: A health care provider is not a covered entity based on his being a workforce member of a health care provider that conducts the standard transactions. Thus, a health care provider may maintain a separate uncovered practice (if he does not engage in standard transactions electronically in connection with that practice), even though the provider may also practice at a hospital which may be a covered entity. However, the Rule does not permit an individual provider to use hybrid entity status to eliminate protections on information when he is not conducting standard transactions. If a health care provider conducts standard transactions electronically on his own behalf, then the protected health information maintained or transmitted by that provider is covered, regardless of whether the information is actually used in such transactions.

Comment: One commenter requested a clarification that employers are not hybrid entities simply because they may be the plan sponsor of a group health plan.

Response: The Department clarifies that an employer is not a hybrid entity simply because it is the plan sponsor of a group health plan. The employer/plan sponsor and group health plan are separate legal entities and, therefore, do not qualify as a hybrid entity. Further, disclosures from the group health plan to the plan sponsor are governed specifically by the requirements of § 164.504(f).

Comment: A few commenters asked the Department to permit a covered entity with multiple types of health care components to tailor notices to address the specific privacy practices within a component, rather than have just one generic notice for the entire covered entity.

Response: Covered entities are allowed to provide a separate notice for each separate health care component, and are encouraged to provide individuals with the most specific notice possible.

2. Group Health Plan Disclosures of Enrollment and Disenrollment Information to Plan Sponsors

December 2000 Privacy Rule. The Department recognized the legitimate need of plan sponsors and employers to access health information held by group health plans in order to carry out essential functions related to the group health plan. 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 a plan sponsor provided that, among other requirements, the plan documents are amended appropriately to reflect and restrict the plan sponsor's uses and disclosures of such information. The Department further determined that there were two situations in which protected health information could be shared between the group health plan and the plan sponsor without individual authorization or an amendment to the plan documents. First, § 164.504(f) permits the group health plan to share summary health information (as defined in § 164.504(a)) with the plan sponsor. Second, a group health plan is allowed to share enrollment or disenrollment information with the plan sponsor without amending the plan documents as required by § 164.504(f). As explained in the preamble to the December 2000 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. However, the second exception was not stated in the regulation text.

March 2002 NPRM. The ability of group health plans to disclose enrollment or disenrollment information without amending the plan documents was addressed only in the preamble to the Privacy Rule. The absence of a specific provision in the regulation text caused many entities to conclude that plan documents would need to be amended for enrollment and disenrollment information to be exchanged between plans and plan sponsors. To remedy this misunderstanding and make its policy clear, the Department proposed to add an explicit exception at § 164.504(f)(1)(iii) to clarify that group health plans (or health insurance issuers or HMOs with respect to group health plans, as appropriate) are permitted to disclose enrollment or disenrollment information to a plan sponsor without meeting the plan document amendment and other related requirements.

Overview of Public Comments. The following discussion provides an overview of the public comment received on this proposal. Additional comments received on this issue are discussed below in the section entitled, ''Response to Other Public Comments.''

Commenters in general supported the proposed modification. Some supported the proposal because it was limited to information about whether an individual is participating or enrolled in a group health plan and would not permit the disclosure of any other protected health information. Others asserted that the modification is a reasonable approach because enrollment and disenrollment information is needed by plan sponsors for payroll and other employment reasons.

Final Modifications. The Department adopts the modification to § 164.504(f)(1)(iii) essentially as proposed. Thus, a group health plan, or

a health insurance issuer or HMO acting for a group health plan, may disclose to a 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. This disclosure can be made without amending the plan documents. In adopting the modification as a final Rule, the Department deletes the phrase ''to the plan sponsor'' that appeared at the end of the proposed new provision, as mere surplusage.

As a result of the modification, summary health information and enrollment and disenrollment information are treated consistently. Under § 164.504(f), as modified, group health plans can share summary health information and enrollment or disenrollment information with plan sponsors without having to amend the plan documents. Section 164.520(a) provides that a fully insured group health plan does not need to comply with the Privacy Rule's notice requirements if the only protected health information it creates or receives is summary health information and/or information about individuals' enrollment in, or disenrollment from, a health insurer or HMO offered by the group health plan. Similarly, in § 164.530(k), the Department exempts fully insured group health plans from many of the administrative requirements in that section if the only protected health information held by the group health plan is summary health information and/or information about individuals' enrollment in, or disenrollment from, a health insurer or HMO offered by the group health plan. Such consistency will simplify compliance with the Privacy Rule.

Response to Other Public Comments

Comment: One commenter stated that there needs to be protection for health information given to group health plans on enrollment forms. In particular, this commenter suggested that the Department include a definition of ''enrollment'' or ''disenrollment'' information that specifies that medical information, such as past or present medical conditions and doctor or hospital visits, is not enrollment information, but rather is individually identifiable health information, and therefore, subject to the Privacy Rule's protections.

Response: Individually identifiable health information received or created by the group health plan for enrollment purposes is protected health information under the Privacy Rule. The modification to § 164.504(f) being adopted in this rulemaking does not affect this policy. The Privacy Rule does not define the information that may be transmitted for enrollment and disenrollment purposes. Rather, the Department in the Transactions Rule has adopted a standard transaction for enrollment and disenrollment in a health plan. That standard (ASC X12N 834, Benefit Enrollment and Maintenance, Version 4010, May 2000, Washington Publishing Company) specifies the required and situationally required data elements to be transmitted as part of such a transaction. While the standard enrollment and disenrollment transaction does not include any substantial clinical information, the information provided as part of the transaction may indicate whether or not tobacco use, substance abuse, or short, long-term, permanent, or total disability is relevant, when such information is available. However, the Department clarifies that, in disclosing or maintaining information about an individual's enrollment in, or disenrollment from, a health insurer or HMO offered by the group health plan, the group health plan may not include medical information about the individual above and beyond that which is required or situationally required by the standard transaction and still qualify for the exceptions for enrollment and disenrollment information allowed under the Rule.

Comment: Several commenters recommended that enrollment and disenrollment information specifically be excluded from the definition of ''protected health information.'' They argued that this change would be warranted because enrollment and disenrollment information do not include health information. They further argued that such a change would help alleviate confusion surrounding the application of the Privacy Rule to employers.

Response: We disagree that enrollment and disenrollment information should be excluded from the definition of ''protected health information.'' Enrollment and disenrollment information fall under the statutory definition of ''individually identifiable health information,'' since it is received or created by a health plan, identifies an individual, and relates to the past, present, or future payment for the provision of health care to an individual. As such, the Department believes there is no statutory basis to exclude such information from the definition of ''protected health information.'' The Department believes that the exception to the requirement for group health plans to amend plan documents that has been added to the Privacy Rule for enrollment and disenrollment information balances the legitimate need that plan sponsors have for enrollment and disenrollment information against the individual's right to have such information kept private and confidential.

Comment: Given that, under § 164.504(f)(2), plan sponsors agree not to use or further disclose protected health information other than as permitted or required by plan documents or ''required by law,'' one commenter requested that the definition of ''required by law'' set forth at § 164.501 should be revised to reflect that it applies not only to covered entities, but also to plan sponsors who are required to report under OSHA or similar laws.

Response: The Department agrees and has made a technical correction to the definition of ''required by law'' in § 164.501 to reflect that the definition applies to a requirement under law that compels any entity, not just a covered entity, to make a use or disclosure of protected health information.

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

1. Consent

December 2000 Privacy Rule. 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 balanced the privacy implications of uses and disclosures for treatment, payment, and health care operations and the need for these core activities to continue. 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. Given public 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 the efficient payment for such health care, the Department's goal is, and has always been, to permit these activities to occur with little or no restriction.

Consistent with this goal, the Privacy Rule published in December 2000 generally provided 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 direct treatment relationships with individuals, such as many physicians, hospitals, and pharmacies, the December 2000 Privacy Rule required such providers to obtain an individual's written consent prior to using or disclosing protected health information for these purposes. The Department designed consent as a one-time, general permission from the individual, which the individual would have had the right to revoke. A health care provider could have conditioned treatment on the receipt of consent. Other covered entities also could have chosen to obtain consent but would have been required to follow the consent standards if they opted to do so.

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 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.

The transition provisions of the Privacy Rule permit covered health care providers that were required to obtain consent to use and disclose protected health information they created or received prior to the compliance date of the Privacy Rule for treatment, payment, or health care operations if they had obtained consent, authorization, or other express legal permission to use or disclose such information for any of these purposes, even if such permission did not meet the consent requirements of the Privacy Rule.

March 2002 NPRM. The Department heard concerns about significant practical problems that resulted from the consent requirements in the Privacy Rule. Covered entities and others provided numerous examples of obstacles that the consent provisions would pose to timely access to health care. These examples extended to various types of providers and various settings. The most troubling, pervasive problem was that health care providers would not have been able to use or disclose protected health information for treatment, payment, or health care operations purposes prior to their initial face-to-face contact with the patient, something which is routinely done today to provide patients with timely access to quality health care. A list of some of the more significant examples and concerns are as follows:

- Pharmacists would not have been able to fill a prescription, search for potential drug interactions, determine eligibility, or verify coverage before the individual arrived at the pharmacy to pick up the prescription if the individual had not already provided consent under the Privacy Rule.
- Hospitals would not have been able to use information from a referring physician to schedule and prepare for procedures before the individual presented at the hospital for such procedure, or the patient would have had to make a special trip to the hospital to sign the consent form.
- Providers who do not provide treatment in person may have been unable to provide care because they would have had difficulty obtaining prior written consent to use protected health information at the first service delivery.
- Emergency medical providers were concerned that, if a situation was urgent, they would have had to try to obtain consent to comply with the Privacy Rule, even if that would be inconsistent with appropriate practice of emergency medicine.
- Emergency medical providers were also concerned that the requirement that they attempt to obtain consent as soon as reasonably practicable after an emergency would have required significant efforts and administrative burden which might have been viewed as harassing by individuals, because these providers typically do not have ongoing relationships with individuals.
- Providers who did not meet one of the consent exceptions were concerned that they could have been put in the untenable position of having to decide whether to withhold treatment when an individual did not provide consent or proceed to use information to treat the individual in violation of the consent requirements.
- The right to revoke a consent would have required tracking consents, which could have hampered treatment and resulted in large institutional providers deciding that it would be necessary to obtain consent at each patient encounter instead.
- The transition provisions would have resulted in significant operational problems, and the inability to access health records would have had an adverse effect on quality activities, because many providers currently are not required to obtain consent for treatment, payment, or health care operations.
- 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 have resulted because they would have had to ask for consent to use or disclose protected health information for treatment, payment, or health care operations, but could have used or disclosed the information for such purposes even if the patient said ''no.''

As a result of the large number of treatment-related obstacles raised by various types of health care providers that would have been required to obtain consent, the Department became concerned that individual fixes would be too complex and could possibly overlook important problems. Instead, the Department proposed an approach designed to protect privacy interests by affording patients the opportunity to engage in important discussions regarding the use and disclosure of their health information through the strengthened notice requirement, while allowing activities that are essential to quality health care to occur unimpeded (see section III.H. of the preamble for a discussion of the strengthened notice requirements).

Specifically, the Department proposed to make the obtaining of consent to use and disclose protected health information for treatment, payment, or health care operations more flexible for 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.

The NPRM included provisions to permit covered entities to obtain consent for uses and disclosures of protected health information for treatment, payment, or health care

operations, if they wished to do so. These provisions would grant providers complete discretion in designing this process. These proposed changes were partnered, however, by the proposal to strengthen the notice provisions to require direct treatment providers to make good faith efforts to obtain a written acknowledgment of receipt of the notice. The intent was to preserve the opportunity to raise questions about the entity's privacy policies that the consent requirements previously provided.

Overview of Public Comments. The following discussion provides an overview of the public comment received on this proposal. Additional comments received on this issue are discussed below in the section entitled, ''Response to Other Public Comments.''

The vast majority of commenters addressed the consent proposal. Most comments fell into three basic categories: (1) Many comments supported the NPRM approach to eliminate the consent requirement; (2) many comments urged the Department to require consent, but make targeted fixes to address workability issues; and (3) some comments urged the Department to strengthen the consent requirement.

The proposed approach of eliminating required consent and making obtaining of consent permissible, at the entity's discretion, was supported by many covered entities that asserted that it would provide the appropriate balance among access to quality health care, administrative burden, and patient privacy. Many argued that the appropriate privacy protections were preserved by strengthening the notice requirement. This approach was also supported by the NCVHS.

The comments received in response to the NPRM continued to raise the issues and obstacles described above, and others. For example, in addition to providing health care services to patients, hospices often provide psychological and emotional support to family members. These consultations often take place long distance and would likely be considered treatment. The consent requirement would make it difficult, or impossible in some circumstances, for hospices to provide these important services to grieving family members on a timely basis. Comments explained that the consent provisions in the Rule pose significant obstacles to oncologists as well. Cancer treatment is referral-based. Oncologists often obtain information from other doctors, hospital, labs, etc., speak with patients by telephone, identify treatment options, and develop preliminary treatment plans, all before the initial patient visit. The prior consent requirement would prevent all of these important preliminary activities before the first patient visit, which would delay treatment in cases in which such delay cannot be tolerated.

Other commenters continued to strongly support a consent requirement, consistent with their views expressed during the comment period in March 2001. Some argued that the NPRM approach would eliminate an important consumer protection and that such a ''radical'' approach to fixing the workability issues was not required. They recommended a targeted approach to fixing each problem, and suggested ways to fix each unintended consequence of the consent requirement, in lieu of removing the requirement to obtain consent.

A few commenters argued for reinstating a consent requirement, but making it similar to the proposal for acknowledgment of notice by permitting flexibility and including a ''good faith'' standard. They also urged the Department to narrow the definition of health care operations and require that de-identified information be used where possible for health care operations.

Finally, a few commenters continued to assert that consent should be strengthened by applying it to more covered entities, requiring it to be obtained more frequently, or prohibiting the conditioning of treatment on the obtaining of consent.

Final Modifications. The Department continues to be concerned by the multitude of comments and examples demonstrating that the consent requirements would result in unintended consequences that would impede the provision of health care in many critical circumstances. We are also concerned that other such unintended consequences may exist which have yet to be brought to our attention. The Department would not have been able to address consent issues arising after publication of this Rule until at least a year had passed from this Rule's publication date due to statutory limitations on the timing of modifications. The Department believes in strong privacy protections for individually identifiable health information, but does not want to compromise timely access to quality health care. The Department also 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 protected health information about him or her.

A review of the comments showed that almost all of the commenters that discussed consent acknowledged that there are unintended consequences of the consent requirement that would interfere with treatment. These comments point toward two potential approaches to fixing these problems. The Department could address these problems by adopting a single solution that would address most or all of the concerns, or could address these problems by adopting changes targeted to each specific problem that was brought to the attention of the Department. One of the goals in making changes to the Privacy Rule is to simplify, rather than add complexity to, the Rule. Another goal is to assure that the Privacy Rule does not hamper necessary treatment. For both of these reasons, the Department is concerned about adopting different changes for different issues related to consent and regulating to address specific examples that have been brought to its attention. Therefore, the options that the Department most seriously considered were those that would provide a global fix to the consent problems. Some commenters provided global options other than the proposed approach. However, none of these would have resolved the operational problems created by a mandatory consent.

The Department also reviewed State laws to understand how they approached uses and disclosures of health information for treatment, payment, or health care operations purposes. Of note was the California Confidentiality of Medical Information Act. Cal. Civ. Code § 56. This law permits health care providers and health plans to disclose health information for treatment, payment, and certain types of health care operations purposes without obtaining consent of the individual. The California HealthCare Foundation conducted a medical privacy and confidentiality survey in January 1999 that addressed consumer views on confidentiality of medical records. The results showed that, despite the California law that permitted disclosures of health information without an individual's consent, consumers in California did not have greater concerns about confidentiality than other health care consumers. This is true with respect to trust of providers and health plans to keep health information private and confidential and the level of access to health information that providers and health plans have.

The Department adopts the approach that was proposed in the NPRM, because it is the only one that resolves the operational problems that have been identified in a simple and uniform manner. First, this Rule strengthens the notice requirements to preserve the opportunity for individuals to discuss privacy practices and concerns with providers. (See section III.H. of the preamble for the related discussion of modifications to strengthen the notice requirements.) Second, the final Rule makes the obtaining of consent to use and disclose protected health information for treatment, payment, or health care operations optional on the part of all covered entities, including providers with direct treatment relationships. A health care provider that has a direct treatment relationship with an individual is not required by the Privacy Rule 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, have regulatory permission for such uses and disclosures. The fact that there is a State law that has been using a similar model for years provides us confidence that this is a workable approach.

Other rights provided by the Rule are not affected by this modification. Although covered entities will not be required to obtain an individual's consent, any uses or disclosures of protected health information for treatment, payment, or health care operations must still be consistent with the covered entity's notice of privacy practices. Also, the removal of the consent requirement applies only 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 or any other requirements for the use or disclosure of protected health information. 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 purposes not otherwise permitted or required by the Privacy Rule. Furthermore, individuals retain the right to request restrictions, in accordance with § 164.522(a). This allows individuals and covered entities to enter into agreements to restrict uses and disclosures of protected health information for treatment, payment, and health care operations that are enforceable under the Privacy Rule.

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

This final Rule allows covered entities that choose to have a consent process complete discretion in designing that process. Prior comments have informed the Department that one consent process and one set of principles will likely be unworkable. Covered entities that choose to obtain consent may rely on industry practices to design a voluntary consent process that works best for their practice area and consumers, but they are not required to do so.

This final Rule effectuates these changes in the same manner as proposed by the NPRM. The consent provisions in § 164.506 are replaced with a new provision at § 164.506(a) that provides regulatory permission for covered entities to use or disclose protected health information for treatment, payment, and health care operations. A new provision is added at § 164.506(b) that permits covered entities to obtain consent if they choose to, and makes clear any such consent process does not override or alter the authorization requirements in § 164.508. Section 164.506(b) includes a small change from the proposed version to make it clearer that authorizations are still required by referring directly to authorizations under § 164.508.

Additionally, this final Rule includes a number of conforming modifications, identical to those proposed in the NPRM, to accommodate the new approach. The most substantive corresponding changes are 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 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 are collapsed into a single provision, and the language is modified to eliminate the consent requirement.

The references in § 164.532 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 are deleted. 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 are not necessary.

This final Rule also includes conforming changes to the definition of ''more stringent'' in § 160.202; the text of § 164.500(b)(1)(v), §§ 164.508(a)(2)(i) and (b)(3)(i), and § 164.520(b)(1)(ii)(B); the introductory text of §§ 164.510 and 164.512, and the title of § 164.512 to eliminate references to required consent.

Response to Other Public Comments

Comment: There were three categories of commenters with respect to the Rule's general approach to consent-those that supported the changes proposed in the NPRM provisions, those that requested targeted changes to the consent requirement, and those that requested that the consent requirement be strengthened.

Many commenters supported the NPRM approach to consent, making consent to use or disclose protected health information for treatment, payment, and health care operations voluntary for all covered entities. These commenters said that this approach provided flexibility for covered entities to address consent in a way that is consistent with their practices. These commenters also stated that the NPRM approach assured that the Privacy Rule would not interfere with or delay necessary treatment.

Those that advocated retaining a consent requirement stated that the NPRM approach would undermine trust in the health care system and that requiring consent before using or disclosing protected health information shows respect for the patient's autonomy, underscores the need to inform the patient of the risks and benefits of sharing protected health information, and makes it possible for the patient to make an informed decision. Many of these commenters suggested that the consent requirement be retained and that the problems raised by consent be addressed through targeted changes or guidance for each issue.

Some suggestions targeted to specific problems were: (1) Fix the problems

related to filling prescriptions by treating pharmacists as providers with indirect treatment relationships or by deeming a prescription to serve as an implied consent; and (2) allow certain uses and disclosures prior to first patient encounter. Some of these commenters argued that certain issues could be addressed through guidance on other provisions in the Rule, rather than a change in the regulation. For example, they suggested that guidance could explain that physicians who take phone calls for one another are part of an organized health care arrangement, or could provide technical assistance about revocations on consent by identifying when a covered entity has taken action in reliance on a consent.

Other suggestions were more general. They included suggestions that the Department: (1) Substitute a good faith effort requirement for the current provisions; (2) provide regulatory permission for certain uses and disclosures of protected heath information prior to first service delivery; (3) permit oral consent with documentation; (4) retain a consent requirement for disclosures, but not uses; (5) retain a consent requirement for payment and operations, but not treatment uses and disclosures; (6) allow individuals to opt out of the consent requirement; (7) allow the consent to apply to activities of referred-to providers, and (8) retain the consent requirement but add flexibility, not exceptions.

The third group of commenters requested that the consent requirement be strengthened. Some requested that the Privacy Rule not permit conditioning of treatment or enrollment on consent for multiple uses and disclosures. Others requested that the consent requirement be extended to covered entities other than providers with direct treatment relationships, such as health plans. Some commenters also asked that the consent be time-limited or be required more frequently, such as at each service delivery.

Response: The Department recognizes that there are some benefits to the consent requirement and has considered all options to preserve the consent requirement while fixing the problems it raises. After examining each of these options, we do not believe that any would address all of the issues that were brought to the Department's attention during the comment process or would be the best approach for regulating this area. For example, the suggestion to treat pharmacists as indirect treatment providers would not be consistent with the current regulatory definition of that term and would not have addressed other referral situations. This approach was also rejected by some pharmacists who view themselves as providing treatment directly to individuals. The suggestion to allow certain uses and disclosures prior to first patient encounter would not address concerns of tracking consents, use of historical data for quality purposes, or the concerns of emergency treatment providers.

The Department desired a global approach to resolving the problems raised by the prior consent requirement, so as not to add additional complexity to the Privacy Rule or apply different standards to different types of direct treatment providers. This approach is consistent with the basic goal of the Rule to provide flexibility as necessary for the standards to work for all sectors of the health care industry.

More global approaches suggested were carefully considered, but each had some flaw or failed to address all of the treatment-related concerns brought to our attention. For example, those who suggested that the Rule be modified to require a good faith effort to obtain consent at first service delivery failed to explain how that approach would provide additional protection than the approach we proposed. The Department also decided against eliminating the consent requirement only for uses and disclosures for treatment, or only for uses of protected health information but not for disclosures, because these options fall short of addressing all of the problems raised. Scheduling appointments and surgeries, and conducting many pre-admission activities, are health care operations activities, not treatment. Retaining the consent requirement for payment would be problematic because, in cases where a provider, such as a pharmacist or hospital, engages in a payment activity prior to face-to-face contact with the individual, it would prohibit the provider from contacting insurance companies to obtain pre-certification or to verify coverage.

Similarly, the suggestion to limit the prior consent requirement to disclosures and not to uses would not have addressed all of the problems raised by the consent requirements. Many of the basic activities that occur before the initial face-to-face meeting between a provider and an individual involve disclosures as well as uses. Like the previous approach, this approach also would prohibit pharmacists and hospitals from contacting insurance companies to obtain pre-certification or verify coverage if they did not have the individual's prior consent to disclose the protected health information for payment. It also would prohibit a provider from contacting another provider to ask questions about the medical record and discuss the patient's condition, because this would be a disclosure and would require consent.

There was a substantial amount of support from commenters for the approach taken in the NPRM. The Department continues to believe that this approach makes the most sense and meets the goals of not interfering with access to quality health care and of providing a single standard that works for the entire health care industry. Therefore, the Department has adopted the approach proposed in the NPRM.

Comment: Some commenters asserted that eliminating the consent requirement would be a departure from current medical ethical standards that protect patient confidentiality and common law and State law remedies for breach of confidentiality that generally require or support patient consent prior to disclosing patient information for any reason. Another commenter was concerned that the removal of the consent requirement from the Privacy Rule will become the de facto industry standard and supplant professional ethical duties to obtain consent for the use of protected health information.

Response: The Privacy Rule provides a floor of privacy protection. State laws that are more stringent remain in force. In order not to interfere with such laws and ethical standards, this Rule permits covered entities to obtain consent. Nor is the Privacy Rule intended to serve as a ''best practices'' standard. Thus, professional standards that are more protective of privacy retain their vitality.

Comment: Some commenters requested that, if the Department adopts the NPRM approach to eliminate the consent requirement for uses and disclosures of protected health information for treatment, payment, or health care operations, the definition of ''health care operations'' should also be narrowed to protect individual expectations of privacy.

Response: We disagree. As stated in the preamble to the December 2000 Privacy Rule, the Department believes that narrowing the definition of ''health care operations'' will place serious burdens on covered entities and impair their ability to conduct legitimate business and management functions.

Comment: Some commenters requested that the regulation text state more specifically that a voluntary consent cannot substitute for an authorization when an authorization is otherwise required under the Privacy Rule.

Response: The Department agrees and modifies the regulation text, at § 164.506(b)(2), to make this clear. As stated in the preamble to the NPRM, the Department intends to enforce strictly the requirement for obtaining an individual's authorization, in accordance with § 164.508, for uses and disclosures of protected health information for purposes not otherwise permitted or required by the Privacy Rule. A consent obtained voluntarily would not be sufficient to permit a use or disclosure which, under the Privacy Rule, requires an authorization or is otherwise expressly conditioned under the Rule. For example, a consent under § 164.506 could not be obtained in lieu of an authorization required by § 164.508 or a waiver of authorization by an IRB or Privacy Board under § 164.512(i) to disclose protected health information for research purposes.

Comment: Some commenters requested that, if the Department decides to allow consent on a voluntary basis, the Privacy Rule include requirements for those covered entities that voluntarily choose to obtain consents.

Response: The goal of the NPRM approach was to enhance flexibility for covered entities by allowing them to design a consent process that best matches their needs. The Department learned over the past year that no single consent process works for all covered entities. In addition, the Department wants to encourage covered entities to adopt a consent process, and is concerned that by prescribing particular rules, it would discourage some covered entities from doing so.

Comment: Some commenters asserted that the consent requirement provides individuals with control because providers may not opt to withhold treatment if a patient refuses consent only for the use or disclosure of protected health information for health care operations.

Response: These commenters may not fully understand the consent requirements in the December 2000 Rule. That requirement did not allow separate consents for use of protected health information for treatment, payment, and health care operations. The only way to allow use of protected health information for treatment but not for health care operations purposes would have been to invoke the right to request restrictions (§ 164.522(a)); the provider could agree or not agree to restrict use and disclosure of protected health information for health care operations. That is also how the Rule will work with these modifications. The Department is not modifying the right to request restrictions.

Comment: Some commenters were confused about the relationship between the proposed changes to the consent provisions and State law. Some were concerned that the Privacy Rule would override State consent laws which provide stronger protections for medical and psychotherapeutic privacy.

Response: The Privacy Rule does not weaken the operation of State laws that require consent to use or disclose health information. The Privacy Rule permits a covered entity to obtain consent to use or disclose health information, and, therefore, presents no barrier to the entity's ability to comply with State law requirements.

Comment: One commenter suggested that the consent requirement be retained to protect victims of domestic violence.

Response: The Department understands the concerns that the Privacy Rule not endanger victims of domestic violence, but we do not believe that eliminating the consent requirement will do so. The Department believes that the provisions that provide real protections to victims of domestic violence in how information is used or disclosed for treatment, payment, and health care operations, are provisions that allow an individual to object to disclosure of directory information and of protected health information to family members or friends involved in the individual's care (*see* § 164.510), that provide an individual the right to request restrictions (*see* § 164.522(a)), and that grant an individual the right to request confidential communications (*see* § 164.522(b)). These provisions are not affected by the changes in this final Rule.

Comment: One commenter asserted that written consent represents a signed agreement between the provider and patient regarding the manner in which covered entities will use and disclose health information in the future, and that the removal of this requirement would shift ''ownership'' of records from patients to doctors and corporate entities.

Response: The Department disagrees with this position. Our research indicates that a signed consent form is most typically treated as a waiver of rights by a patient and not as a binding agreement between a provider and a patient. Further, many States have laws assigning the ownership of records, apart from any consent requirements. The Privacy Rule does not address, and is not intended to affect, existing laws governing the ownership of health records.

Comment: A few commenters claimed that the signed notice of a provider's privacy policy is meaningless if the individual has no right to withhold consent and the NPRM approach would reinforce the fact that individuals have no say in how their health information is used or disclosed.

Response: The Department disagrees. The individual's options under the consent requirement established by the Privacy Rule published in December 2000 and the voluntary consent and strengthened notice provisions adopted by this Rule are the same. Under the previous Rule, a patient who disagreed with the covered entity's information practices as stated in the notice could withhold consent and not receive treatment, or could sign the consent form and obtain treatment despite concerns about the information practices. The patient could request that the provider restrict the use and/or disclosure of the information. Under the Rule as modified, a patient who disagrees with the covered entity's information practices as stated in the notice, can choose not to receive treatment from that provider, or can obtain treatment despite concerns about the information practices. The patient can request that the provider restrict the use and/or disclosure of the information. The result, for the patient, is the same.

Comment: One commenter requested clarification with respect to the effect of a revocation of voluntary consent and whether agreed-to restrictions must be honored.

Response: The final Rule is silent as to how a covered entity handles the revocation of a voluntary consent under § 164.506(b)(1). The Rule provides the covered entity that chooses to adopt a consent process discretion to design the process that works for that entity.

The change to the consent provision in the Privacy Rule does not affect the right of an individual under § 164.522(a) to request restrictions to a use or disclosure of protected health information. While a covered entity is not required to agree to such restrictions, it must act in accordance with any restriction it does agree to. Failure of a covered entity to act in accordance with an agreed-to restriction is a violation of the Rule.

Comment: Commenters asked the Department to rename consent to ''consent for information use'' to reduce confusion with consent for treatment.

Response: In order to clear up confusion between informed consent for treatment, which is addressed by State law, and consent to use or disclose protected health information under the

Privacy Rule, we changed the title of § 164.506(b) from ''Consent permitted'' to ''Consent for uses and disclosures of information permitted.'' The Privacy Rule does not affect informed consent for treatment.

Comment: A few commenters requested that the Department modify the regulation to state that de-identified information should be used for health care operations where possible.

Response: The Department continues to encourage covered entities to use de-identified information wherever possible. As the Department has made this position clear in the preambles to both the December 2000 Privacy Rule and the March 2002 NPRM, as well as in this preamble, we do not believe that it is necessary to modify the regulation to include such language. Further, the minimum necessary requirements, under §§ 164.502(b)(2) and 164.514(d), already require a covered entity to make reasonable efforts to limit protected health information used for health care operations and other purposes to the minimum necessary to accomplish the intended purpose, which may, in some cases, be de-identified information.

Comment: One commenter requested that the Privacy Rule state that consent is not required for provider-to-provider communications.

Response: Prior to these final modifications, the consent requirements of the Privacy Rule would have required a provider to obtain written consent to disclose protected health information to another provider for treatment purposes—which could have interfered with an individual's ability to obtain timely access to quality care. This is one reason the Department has eliminated the consent requirement for treatment, payment, and health care operations. Providers will not need a patient's consent to consult with other providers about the treatment of a patient. However, if a provider is disclosing protected health information to another provider for purposes other than treatment, payment, or health care operations, an authorization may be required under § 164.508 (*e.g.*, generally, disclosures for clinical trials would require an authorization).

Comment: One commenter asserted that, without a consent requirement, nothing will stop a health plan from demanding a patient's mental health records as a condition of payment for physical therapy.

Response: The Department does not agree that the former consent requirement is the relevant standard with respect to the activities of the health plan that concern the commenter. Rather, the Transactions Rule and the minimum necessary standard of the Privacy Rule prescribe and limit the health information that may be disclosed as part of payment transactions between health plans and health care providers. Although a health plan may request additional information to process a specific claim, in addition to the required and situational elements under the Transactions Rule, the request must comply with the Privacy Rule's minimum necessary requirements. In this example, the health plan can only request mental health records if they are reasonably necessary for the plan to process the physical therapy claim.

2. Disclosures for Treatment, Payment, or Health Care Operations of Another Entity

December 2000 Privacy Rule. The Privacy Rule permits a covered entity to use and disclose protected health information for treatment, payment, or health care operations. For treatment purposes, the Rule generally allows protected health information to be shared without restriction. The definition of ''treatment'' incorporates the necessary interaction of more than one entity. In particular, the definition of ''treatment'' includes the 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 purposes 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, as published in December 2000, generally limited a covered entity's uses and disclosures of protected health information to those that were necessary for its own payment and health care operations activities. This limitation was explicitly stated in the December 2000 preamble discussions of the definitions of ''payment'' and ''health care operations.'' 65 FR 82490, 82495. The Privacy Rule also provided 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* 45 CFR 164.506(a)(5) and 164.508(e).

March 2002 NPRM. Since the publication of the December 2000 Rule, a number of commenters raised specific concerns with the restriction that a covered entity may not disclose protected health information for another entity's payment and health care operations activities, absent an authorization. These commenters presented a number of examples where such a restriction would impede the ability of certain 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, for example, the Department heard concerns of ambulance service providers who explained that they normally receive the information they need to obtain payment for their treatment services from the hospital emergency departments to which they transport their patients. They explained that it is usually not possible for the ambulance service provider to obtain such information directly from the individual, nor is it always practicable or feasible for the hospital to obtain the individual's authorization to provide payment information to the ambulance service provider. This disclosure of protected health information from the hospital to the ambulance service provider was not permitted under the December 2000 Privacy Rule without an authorization from the patient, because it was a disclosure by the hospital for the payment activities of the ambulance service provider.

Commenters also were concerned about situations in which covered entities outsource their billing, claims, and reimbursement functions to accounts receivable management companies. These collectors often attempt to recover payments from a patient on behalf of multiple health care providers. Commenters were concerned that the Privacy Rule would prevent these collectors, as business associates of multiple providers, from using a patient's demographic information received from one provider to facilitate collection for another provider's payment.

With regard to health care operations, the Department also received comments about the difficulty that the Privacy Rule would 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' quality-related activities, accreditation, and performance measures, such as 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.

The NCVHS, in response to public testimony on this issue at its August 2001 hearing, also recommended that the Department amend the Privacy Rule to allow for uses and disclosures for quality-related activities among covered entities, without the individual's written authorization.

Based on these concerns, the Department proposed to modify § 164.506 to permit a covered entity to disclose protected health information for the payment activities of another covered entity or any health care provider, and also for certain types of health care operations of another covered entity. The proposal would broaden the uses and disclosures that are permitted without authorization 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 the individual.

Specifically, the Department proposed the following. First, the Department proposed to add to § 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 permission.

Second, the Department proposed to include language in § 164.506(c)(2) 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, whether or not that specialist is also a covered entity. No authorization would be required.

Third, the Department proposed to include language in § 164.506(c)(3) to permit a covered entity to disclose protected health information to another covered entity or any health care provider for the payment activities of that entity. The Department recognized that not all health care providers who need protected health information to obtain payment are covered entities, and, therefore, proposed to allow disclosures of protected health information to both covered and non-covered health care providers. In addition, the Department proposed a conforming change to delete the word ''covered'' in paragraph (1)(ii) of the definition of ''payment,'' to permit disclosures to non-covered providers for their payment activities.

The Department also proposed to limit disclosures under this provision to those health plans that are covered by the Privacy Rule. However, the Department solicited comment on whether plans that are not covered by the Privacy Rule would be able to obtain the protected health information that they need for payment purposes.

Fourth, in § 164.506(c)(4), the Department proposed to permit a covered entity to disclose protected health information about an individual to another covered entity for specified health care operations purposes of the covered entity that receives the information, provided that both entities have a relationship with the individual. This proposed expansion was limited in a number of ways. 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. The Department proposed this limitation because it recognized that ''health care operations'' is a broad term and that individuals are less aware of the business-related activities that are part of health care operations than they are of treatment- or payment-related activities. 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. The proposed provision was intended to allow information to flow from one covered entity to another for activities important to providing quality and effective health care.

The proposal would have applied only to disclosures of protected health information to other covered entities. By limiting such disclosures to those entities that are required to comply with the Privacy Rule, the Department intended to ensure that the protected health information remained protected. The Department believed 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.

Further, such disclosures would be permitted only to the extent that each entity has, or had, a relationship with the individual who is the subject of the information being disclosed. Where the relationship between the individual and the covered entity has ended, a disclosure of protected health information about the individual would be allowed only if related to the past relationship. The Department believed that this limitation would be necessary in order to further protect the privacy expectations of the individual.

The proposal made clear that these provisions would not eliminate a covered entity's responsibility to apply the Privacy Rule's minimum necessary provisions to both the disclosure of and request for protected health information for payment and health care operations purposes. In addition, the proposal strongly encouraged the use of de-identified information, wherever feasible.

While the Department stated that it believed it had struck the right balance with respect to the proposed modification for disclosures for health care operations, the Department was aware that the proposal could pose barriers to disclosures for quality-related health care operations to health plans and health care providers that are not covered entities, or to entities that do not have a relationship with the individual. Therefore, the preamble referred commenters to the Department's request for comment on an approach that would permit for any health care operations purposes the disclosure of protected health information that does not contain direct identifiers, subject to a data use or similar agreement.

In addition, related to the above modifications and in response to comments evidencing confusion on this matter, the Department also proposed to clarify that covered entities participating in an organized health care arrangement (OHCA) may share protected health information for the health care operations of the OHCA (§ 164.506(c)(5)). The Department also proposed 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).

Overview of Public Comments. The following discussion provides an overview of the public comment received on this proposal. Additional

comments received on this issue are discussed below in the section entitled, ''Response to Other Public Comments.''

The Department received a number of comments on its proposal to permit a covered entity to disclose protected health information for the payment and health care operations activities of other entities.

Most of the commenters who addressed the Department's proposed clarification regarding treatment expressed support for the clarification. Also, the majority of commenters supported, either wholly or in part, the Department's proposal to expand the payment and health care operations disclosures that would be permitted.

Most commenters generally were supportive of the Department's proposed approach regarding disclosures for payment. A number of commenters stated that the proposed expansion is important to facilitate coordination of benefits for many patients who have multiple sources of payment for prescription drugs. One commenter, however, requested that the Department narrow its proposed language to address only those problems specifically described in the preamble, that is, payment issues faced by ambulance providers and collection agencies that are business associates of multiple health care providers. This commenter stated that, at the very least, covered entities should be required to obtain assurances from non-covered providers, prior to disclosure of protected health information, that the recipient will not use protected health information for any other purpose or disclose it to others. Another commenter remarked that the proposal to limit disclosures only to another covered entity or any health care provider may impede disclosures to reinsurers that are not covered entities.

While most commenters supported expanding disclosures for health care operations, many requested that the Department modify the proposal in a number of ways. For example, a number of health plans and others requested that the Department eliminate the condition that both covered entities have a relationship with the individual. Some of these commenters explained that such a restriction would impede some fraud and abuse activities, credentialing investigations, and quality assurance research and outcome studies. Some commenters asked that the Department clarify that the condition that both covered entities have a relationship with the individual would not be limited to a current relationship, but also would include a past relationship with the individual.

In addition, many commenters requested that the Department expand the proposed provision to allow for disclosures for any type of health care operation of another covered entity, or at least additional activities beyond those specified in the proposal. Some health plans commented that they may need information from a health care provider in order for the health plan to resolve member or internal grievances, provide customer service, arrange for legal services, or conduct medical review or auditing activities. A number of commenters requested that the proposal be expanded to allow for disclosures for another covered entity's underwriting or premium rating.

Some commenters also requested that the Department expand the provision to allow for disclosures to non-covered entities. In particular, a number of these commenters urged that the Department allow disclosures to non-covered insurers for fraud and abuse purposes. Some of these commenters specifically requested that the Department allow for disclosures to affiliated entities or non-health care components of the covered entity for purposes of investigating fraud and abuse. A few commenters requested that the Rule allow for disclosures to a non-covered health care provider for that provider's operations. For example, it was explained that an independent emergency services provider, who is not a covered entity and who often asks for outcome information on patients it has treated and transported to a facility because it wants to improve care, would be unable to obtain such information absent the individual's authorization.

Some commenters were generally opposed to the proposed expansion of the disclosures permitted under the Rule for health care operations purposes, viewing the proposal as a weakening of the Privacy Rule. One of these commenters urged the Department to implement a targeted solution allowing disclosures for only those activities specifically identified as problematic in the preamble, instead of allowing disclosures for all activities that fall within certain paragraphs within the definition of ''health care operations.''

Final Modifications. In this final Rule, the Department adopts its proposal to allow covered entities to disclose protected health information for the treatment, payment, and certain health care operations purposes of another entity. Specifically, the final Rule at § 164.506(c):

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

(2) Clarifies that a covered entity may use or disclose protected health information for the treatment activities of any health care provider.

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

(4) Permits a covered entity to disclose protected health information to another covered entity for the health care operations activities of the entity that receives the information, if each entity either has or had a relationship with the individual who is the subject of the information, the protected health information pertains to such relationship, and the disclosure is:

(i) For a purpose listed in paragraphs (1) or (2) of the definition of ''health care operations,'' which includes quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, case management and care coordination, conducting training programs, and accreditation, licensing, or credentialing activities; or

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

(5) Clarifies that 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.

Based on the comments received, the Department believes that the above provisions strike the appropriate balance between meeting an individual's privacy expectations and meeting a covered entity's need for information for reimbursement and quality purposes. The Department also clarifies that disclosures pursuant to the above provisions may be made to or by a business associate of a covered entity.

In § 164.506(c)(2), in response to a comment, the Department deletes the word ''another'' before ''health care provider'' to eliminate any implication that the disclosing entity must also be a health care provider.

With respect to payment, the majority of commenters were supportive of the Department's proposal. In response to those commenters who expressed support for the proposal because it would facilitate coordination of benefits, the Department clarifies that the definition of ''payment'' in the

Privacy Rule allows for uses and disclosures necessary for coordination of benefits. The new language may, however, reinforce that uses and disclosures for such purposes are permitted under the Rule.

The Department does not believe, as suggested by one commenter, that a targeted approach, one that would address only the problems raised by the ambulance providers and collection agencies, is a practical solution to these problems. The Department believes that these problems may apply in other situations. For example, an indirect treatment provider, such as a pathologist, may need to obtain health coverage information about an individual for billing purposes from the hospital to which the pathologist provided services. If the Department addressed only these discrete scenarios in this final modification, each additional similar problem that arises would require another rulemaking, which would, in and of itself, create a problem because the Department can change a standard only once per year. In addition, by creating special rules to address multiple, distinct circumstances, the Department would have created a substantially more complicated policy for covered entities to follow and implement.

The suggestion that the Department require a covered entity to obtain assurances from non-covered providers, prior to disclosure of protected health information for payment purposes, that the recipient will not use protected health information for any other purpose or disclose it to others, similarly would add a layer of complexity to payment disclosures. Such a requirement would encumber these communications and may interfere with the ability of non-covered health care providers to be paid for treatment they have provided. Moreover, the Privacy Rule requires a covered entity to apply the minimum necessary standard to disclosures for a non-covered provider's payment purposes. Thus, a non-covered provider will receive only the minimum information reasonably necessary for such purposes. Accordingly, the Department believes the final Rule appropriately and practically addresses the issue.

In response to the comment that the proposal may impede disclosures to reinsurers who are not covered entities, the Department clarifies that disclosures to obtain payment under a contract for reinsurance explicitly are permitted as part of the definition of ''payment,'' regardless of whether the reinsurer is a covered entity. Similarly, disclosures for the purposes of ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care are explicitly permitted as part of the definition of ''health care operations,'' also without regard to whether the reinsurer is a covered entity. *See* the definitions of ''payment'' and ''health care operations'' in § 164.501.

With respect to disclosures for the health care operations of another covered entity, the Department continues to believe that the condition that both entities have a relationship with the individual is appropriate to balance an individual's privacy expectations with a covered entity's need for the information. The Department clarifies that a covered entity, prior to making a disclosure allowed under this requirement, is permitted to communicate with another covered entity as necessary to determine if this condition has been met. Additionally, in response to comments, the Department adds language to § 164.506(c)(4) to make clear that the condition that both covered entities have a relationship with the individual is not limited to a current relationship. Where the relationship between the covered entity and the individual has ended, a disclosure of protected health information about the individual is permitted to the extent the disclosure is related to the past relationship. For example, the final Rule would permit a health care provider to disclose protected health information to a health plan for HEDIS purposes, even if the individual no longer was covered by the health plan, provided that the period for which information is needed overlaps with the period for which the individual was enrolled in the health plan.

In response to commenters who were concerned that this condition would impede certain health care operations activities where the covered entity may not have a relationship with the individual, the Department notes that the new limited data set provisions in § 164.514(e) are intended to provide a mechanism for disclosures of protected health information for quality and other health care operations where the covered entity requesting the information does not have a relationship with the individual. Under those provisions, the final modifications permit a covered entity to disclose protected health information, with direct identifiers removed, for any health care operations activities of the entity requesting the information, subject to a data use agreement. Additionally, as clarified by § 164.506(c)(5), covered entities that participate in an OHCA may share protected health information for the health care operations of the OHCA, without the condition that each covered entity have a relationship with the individual who is the subject of the information. The Department believes that such provisions provide adequate avenues for covered entities to obtain the information they need for health care operations activities, without eliminating appropriate privacy protections and conditions on such disclosures.

The Department also was not persuaded by the comments that the proposal should be broadened to allow disclosures for other types of health care operations activities, such as resolution of internal grievances, customer service, or medical review or auditing activities. The Department believes that the provisions at § 164.506(c)(5), which permit covered entities that participate in an OHCA to share information for any health care operations activities of the OHCA, adequately provides for such disclosures. For example, a health plan and the health care providers in its network that participate as part of the same OHCA are permitted to share information for any of the activities listed in the definition of ''health care operations.'' The Department understands the need for entities participating in these joint arrangements to have shared access to information for health care operations purposes and intended the OHCA provisions to provide for such access. Where such a joint arrangement does not exist and fully identifiable health information is needed, one covered entity may disclose protected health information for another covered entity's health care operations pursuant to an individual's authorization as required by § 164.508. In addition, as described above, a covered entity also may disclose protected health information as part of a limited data set, with direct identifiers removed, for such purposes, as permitted by § 164.514(e).

With respect to underwriting and premium rating, a few commenters raised similar concerns that the Department's proposal to expand the disclosures permitted under health care operations would not allow for the disclosures between a health insurance issuer and a group health plan, or the agent or broker as a business associate of the plan, needed to perform functions related to supplementing or replacing insurance coverage, such as to solicit bids from prospective issuers. The Department clarifies that, if more than summary health information is needed for this purpose, paragraphs (3), (4), and (5) of the definition of ''organized health

care arrangement'' may permit the disclosure. These provisions define the arrangements between group health plans and their health insurance issuers or HMOs as OHCAs, which are permitted to share information for each other's health care operations. Such disclosures also may be made to a broker or agent that is a business associate of the health plan. The Department clarifies that the OHCA provisions also permit the sharing of protected health information between such entities even when they no longer have a current relationship, that is, when a group health plan needs protected health information from a former issuer. The Department, therefore, does not believe that a broadening of the provisions under § 164.506(c)(4), to allow disclosures of protected health information for other types of health care operations activities, is warranted.

The final Rule also adopts the condition proposed in the NPRM that disclosures for these health care operations may be made only to another covered entity. The Department continues to consider such a condition necessary to appropriately balance an individual's privacy interests with entities' needs for the information. The Department was not convinced by the commenters who urged that this condition needed to be eliminated to allow for disclosures to non-covered health care providers or third parties. The Department believes that permitting disclosures of protected health information to a non-covered provider for that provider's treatment and payment purposes is warranted and appropriate so as not to impede such core activities. However, given that an individual's health information will no longer be protected when it is disclosed to a non-covered provider, the Department does not consider disclosures for a non-covered provider's health care operations to warrant similar consideration under the Rule. Moreover, this final Rule at § 164.514(e) permits a covered entity to disclose a limited data set, with direct identifiers removed, to a non-covered provider for any of the provider's health care operations purposes, without individual authorization.

Also, the Department believes that expanding the provision to allow disclosures to a third party for any of the third party's business operations would severely weaken the Privacy Rule and essentially negate the need for individual authorization. With respect to those commenters who urged the Department to permit disclosures to non-health care components of a hybrid entity or to an affiliated entity for the purposes of investigating fraud and abuse, the Department's position is that disclosures to a non-health care component within a hybrid entity or to a non-covered affiliated entity present the same privacy risks as do disclosures to a non-covered entity. The Privacy Rule, therefore, permits such disclosures only to the same extent the disclosures are permitted to a separate entity. This policy is further explained in section III.C.1. regarding hybrid entities.

Lastly, the Department believes that the final Rule does in fact implement a targeted solution to the problems previously identified by commenters, by allowing disclosures for only quality-related and fraud and abuse activities. The Department does not believe further limiting such disclosures to only certain activities within paragraphs (1) and (2) of the definition of ''health care operations'' is practical or appropriate. The Department is aware of the important role that these quality-related activities play in ensuring that individuals have access to quality health care. Covered entities have a legitimate need for protected health information in order to conduct these quality activities, regardless of whether such information is used for HEDIS purposes or for training. Moreover, as described above, the final Rule retains a number of conditions on such disclosures that serve to protect an individual's privacy interests and expectations. In addition, the Privacy Rule requires that the minimum necessary standard be applied to both covered entities' requests for and disclosures of protected health information for such purposes.

Response to Other Public Comments

Comment: One commenter urged that the Department permit disclosures among participants in an OHCA only when their privacy notices (or any joint notice they issue) informs individuals of this possibility.

Response: The Privacy Rule requires the joint notice of an OHCA to reflect the fact that the notice covers more than one covered entity and that, if applicable, the covered entities participating in the OHCA will share protected health information with each other, as necessary to carry out treatment, payment, or health care operations relating to the OHCA. *See* § 164.520(d). Where the participants of an OHCA choose to have separate notices, such notices must reflect and describe in sufficient detail the particular uses and disclosures that each covered entity may make to place the individual on notice. This detail should include disclosures to other members of an OHCA, where appropriate.

Comment: Another commenter requested clarification as to whether a covered entity (such as an HMO) is permitted to disclose protected health information for payment and health care operations both to the group health plan and to the plan's third party administrator or plan sponsor. The commenter stated that it was not clear from the proposal whether a covered entity could share protected health information directly with another covered entity's business associate.

Response: The Department clarifies that, if the Rule permits a covered entity to share protected health information with another covered entity, the covered entity is permitted to disclose protected health information directly to a business associate acting on behalf of that other covered entity. This is true with respect to all of the Rule's provisions. Also, an HMO may disclose protected health information to a group health plan, or a third party administrator that is a business associate of the plan, because the relationship between the HMO and the group health plan is defined as an OHCA for purposes of the Rule. See § 164.501, definition of ''organized health care arrangement.'' The group health plan (or the HMO with respect to the group health plan) may disclose protected health information to a plan sponsor in accordance with § 164.504(f).

Comment: Several commenters requested that the Department expand the definition of ''payment'' to include disclosures to a responsible party. Additionally, these commenters urged that the Department permit covered entities (and their business associates) to use and disclose protected health information as permitted by other law, rather than only as required by law. These commenters were concerned that the Privacy Rule would impede the ability of first-party billing companies, collection agencies, and accounts receivable management companies to continue to bill and communicate, on behalf of a health care provider, with the responsible party on an account when that person is different from the individual to whom health care services were provided; report outstanding receivables owed by the responsible party on an account to a credit reporting agency; and perform collection litigation services.

Response: The Department does not believe a modification to the definition of ''payment'' is necessary. The Privacy Rule permits a covered entity, or a business associate acting on behalf of a covered entity (*e.g.,* a collection agency),

to disclose protected health information as necessary to obtain payment for health care, and does not limit to whom such a disclosure may be made. See the definition of ''payment'' in § 164.501. Therefore, a collection agency, as a business associate of a covered entity, is permitted to contact persons other than the individual to whom health care is provided as necessary to obtain payment for such services.

Regarding the commenters' concerns about collection or payment activities otherwise permitted by law, the Department clarifies that the Privacy Rule permits covered entities to use and disclose protected health information as required by other law, or as permitted by other law provided that such use or disclosure does not conflict with the Privacy Rule. For example, the Privacy Rule permits a collection agency, as a business associate of a covered health care provider, to use and disclose protected health information as necessary to obtain reimbursement for health care services, which could include disclosures of certain protected health information to a credit reporting agency, or as part of collection litigation. See the definition of ''payment'' in § 164.501.

The Department notes, however, that a covered entity, and its business associate through its contract, is required to reasonably limit the amount of information disclosed for such purposes to the minimum necessary, where applicable, as well as abide by any reasonable requests for confidential communications and any agreed-to restrictions as required by the Privacy Rule.

Comment: One commenter asked that the Department clarify that disclosure by an eye doctor to confirm a contact prescription received by a mail-order contact company is treatment.

Response: The Department agrees that disclosure of protected health information by an eye doctor to a distributor of contact lenses for the purpose of confirming a contact lens prescription is treatment and is permissible under § 164.506. In relevant part, treatment is defined by the Privacy Rule as ''the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party * * *'' Health care is defined, in part, as ''care, services, or supplies related to the health of an individual. Health care includes * * * Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.'' Therefore, the dispensing of contact lenses based on a prescription is health care and the disclosure of protected health information by a provider to confirm a prescription falls within the provision, coordination, or management of health care and related services and is a treatment activity.

E. Uses and Disclosures for Which Authorization Is Required

1. Restructuring Authorization

December 2000 Privacy Rule. The Privacy Rule requires individual authorization for uses and disclosures of protected health information for purposes that are not otherwise permitted or required under the Rule. To ensure that authorizations are informed and voluntary, the Rule prohibits, with limited exceptions, covered entities from conditioning treatment, payment, or eligibility for benefits or enrollment in a health plan, on obtaining an authorization. The Rule also permits, with limited exceptions, individuals to revoke an authorization at any time. Additionally, the Rule sets out core elements that must be included in any authorization. These elements are intended to provide individuals with the information they need to make an informed decision about giving their authorization. This information includes specific details about the use or disclosure, and provides the individual fair notice about his or her rights with respect to the authorization and the potential for the information to be redisclosed. Additionally, the authorization must be written in plain language so individuals can read and understand its contents. The Privacy Rule required that authorizations 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 another entity to disclose protected health information to the covered entity requesting the authorization to carry out treatment, payment, or health care operations; and in § 164.508(f), for authorizations requested by a covered entity for research that includes treatment of the individual.

March 2002 NPRM. Various issues were raised regarding the authorization requirements. Commenters claimed the authorization provisions were too complex and confusing. They alleged that the different sets of implementation specifications were not discrete, creating the potential for the implementation specifications for specific circumstances to conflict with the required core elements. Some covered entities were confused about which authorization requirements they should implement in any given circumstance. Also, although the Department intended to permit insurers to obtain necessary protected health information during contestability periods under State law, the Rule did not provide an exception to the revocation provision when other law provides an insurer the right to contest an insurance policy.

To address these issues, the Department proposed to simplify the authorization provisions by consolidating the implementation specifications into a single set of criteria under § 164.508(c), thus eliminating paragraphs (d), (e), and (f) which contained separate implementation specifications. Under the proposal, 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 proposal also included new language to clarify that when individuals initiate an authorization for their own purposes, the purpose may be described as ''at the request of the individual.''

In the NPRM, the Department proposed that § 164.508(c)(2) require authorizations to contain the following required 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 redisclosed by the recipient.

Also under the proposal, covered entities would be required to obtain an authorization to use or disclose protected health information for marketing purposes, and to disclose in such authorizations any direct or indirect remuneration the covered entity would receive from a third party as a result of obtaining or disclosing the protected health information. The other proposed changes regarding marketing are discussed in section III.A.1. of the preamble.

The NPRM proposed a new exception to the revocation provision at § 164.508(b)(5)(ii) for authorizations obtained as a condition of obtaining insurance coverage when other law gives the insurer the right to contest the policy. Additionally, the Department proposed that the exception to permit conditioning payment of a claim on obtaining an authorization be deleted, since the proposed provision to permit the sharing of protected health information for the payment activities of another covered entity or a health care provider would eliminate the need for an authorization in such situations.

Finally, the Department proposed modifications at § 164.508(a)(2)(i)(A), (B), and (C), to clarify its intent that the proposed provisions for sharing protected health information for the treatment, payment, or health care operations of another entity would not apply to psychotherapy notes.

There were a number of proposed modifications concerning authorizations for research purposes. Those modifications are discussed in section III.E.2. of the preamble.

Overview of Public Comments. The following discussion provides an overview of the public comment received on this proposal. Additional comments received on this issue are discussed below in the section entitled, ''Response to Other Public Comments.''

There was overwhelming support for the proposed modifications. Overall, supporters were of the opinion that the consolidation and simplification would promote efficiency, simplify compliance, and reduce confusion. Many commenters claimed the changes would eliminate barriers to quality health care. Some commenters claimed the proposed modifications would make the authorization process easier for both providers and individuals, and one commenter said they would make authorizations easier to read and understand. A number of commenters stated the changes would not have adverse consequences for individuals, and one commenter noted the proposal would preserve the opportunity for individuals to give a meaningful authorization.

However, some of the proponents suggested the Department go further to ease the administrative burden of obtaining authorizations. Some urged the Department to eliminate some of the required elements which they perceived as unnecessary to protect privacy, while others suggested that covered entities should decide which elements were relevant in a given situation. Some commenters urged the Department to retain the exception to the prohibition on conditioning payment of a claim on obtaining an authorization. These commenters expressed fear that the voluntary consent process and/or the right to request restrictions on uses and disclosures for treatment, payment, or health care operations might prevent covered entities from disclosing protected health information needed for payment purposes, or providers may be reluctant to cooperate in disclosures for payment purposes based on inadequately drafted notices.

Comments were divided on the proposed requirement to disclose remuneration in marketing authorizations. Recommendations ranged from requiring the disclosure of remuneration on all authorizations, to eliminating the requirement altogether.

Final Modifications. In the final modifications, the Department adopts the changes proposed in the NPRM. Since the modifications to the authorization provision are comprehensive, the Department is publishing this section in its entirety so that it will be easier to use and understand. Therefore, the preamble addresses all authorization requirements, and not just those that were modified.

In § 164.508(a), covered entities are required to obtain an authorization for uses and disclosures of protected health information, unless the use or disclosure is required or otherwise permitted by the Rule. Covered entities may use only authorizations that meet the requirements of § 164.508(b), and any such use or disclosure will be lawful only to the extent it is consistent with the terms of such authorization. Thus, a voluntary consent document will not constitute a valid permission to use or disclose protected health information for a purpose that requires an authorization under the Rule.

Although the requirements regarding uses and disclosures of psychotherapy notes are not changed substantively, the Department made minor changes to the language in paragraph (a)(2) to clarify that a covered entity may not use or disclose psychotherapy notes for purposes of another covered entity's treatment, payment, or health care operations without obtaining the individual's authorization. However, covered entities may use and disclose psychotherapy notes, without obtaining individual authorization, to carry out its own limited treatment, payment, or health care operations as follows: (1) Use by the originator of the notes for treatment, (2) use or disclosure for the covered entity's own training programs for its mental health professionals, students, and trainees, and (3) use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual.

Section 164.508(a)(3) requires covered entities to obtain an authorization to use or disclose protected health information for marketing purposes, with two exceptions. The authorization requirements for marketing and the comments received on these provisions are discussed in detail in section III.A.1. of the preamble.

If the marketing involves any direct or indirect remuneration to the covered entity from a third party, the authorization must state that fact. The comments on this requirement also are discussed in section III.A.1. of the preamble. However, a statement concerning remuneration is not a required notification for other authorizations. Such a statement was never required for all authorizations and the Department believes it would be most meaningful for consumers on authorizations for uses and disclosures of protected health information for marketing purposes. Some commenters urged the Department to require remuneration statements on research authorizations. The Department has not done so because the complexity of such arrangements would make it difficult to define what constitutes remuneration in the research context. Moreover, to require covered entities to disclose remuneration by a third party on authorizations for research would go beyond the requirements imposed in the December 2000 Rule, which did not require such a disclosure on authorizations obtained for the research of a third party. The Department believes that concerns regarding financial conflicts of interest that arise in research are not limited to privacy concerns, but also are important to the objectivity of research and to protecting human subjects from harm. Therefore, in the near future, the Department plans to issue guidance for the research community on this important topic.

Pursuant to § 164.508(b)(1), an authorization is not valid under the Rule unless it contains all of the

required core elements and notification statements, which are discussed below. Covered entities may include additional, non-required elements so long as they are not inconsistent with the required elements and statements. The language regarding defective authorizations in § 164.508(b)(2) is not changed substantively. However, some changes are made to conform this paragraph to modifications to other parts of the authorization provision, as well as other sections of the Rule. An authorization is not valid if it contains any of the following defects: (1) The expiration date has passed or the expiration event has occurred, and the covered entity is aware of the fact, (2) any of the required core elements or notification statements are omitted or incomplete, (3) the authorization violates the specifications regarding compounding or conditioning authorizations, or (4) the covered entity knows that material information in the authorization is false.

In § 164.508(b)(3) regarding compound authorizations, the requirements for authorizations for purposes other than research are not changed. That is, authorizations for use or disclosure of psychotherapy notes may be combined only with another authorization for the use or disclosure of psychotherapy notes. Other authorizations may be combined, unless a covered entity has conditioned the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits on one of the authorizations. A covered entity generally may not combine an authorization with any other type of document, such as a notice of privacy practices or a written voluntary consent. However, there are exceptions for research authorizations, which are discussed in section III.E.2. of the preamble.

Section 164.508(b)(4) prohibits the conditioning of treatment, payment, enrollment in a health plan, or eligibility for benefits on obtaining an authorization, with a few exceptions. The exceptions to this requirement for research-related treatment, eligibility for benefits and enrollment in a health plan, and health care solely for creating protected health information for disclosure to a third party are not changed. Moreover, the Department eliminates the exception to the prohibition on conditioning payment of a claim on obtaining an authorization. Although some insurers urged that this conditioning authority be retained to provide them with more collection options, the Department believes this authorization is no longer necessary because we are adding a new provision in § 164.506 that permits covered entities to disclose protected health information for the payment purposes of another covered entity or health care provider. Therefore, that exception has been eliminated.

Section 164.508(b)(5) provides individuals the right to revoke an authorization at any time in writing. The two exceptions to this right are retained, but with some modification. An individual may not revoke an authorization if the covered entity has acted in reliance on the authorization, or if the authorization was obtained as a condition of obtaining insurance coverage and other law gives the insurer the right to contest the claim or the policy itself. The Department adopts the proposed modification to the latter exception so that insurers can exercise the right to contest an insurance policy under other law. Public comment was generally supportive of this proposed modification.

Section 164.508(b)(6) requires covered entities to document and retain authorizations as required under § 164.530(j). This requirement is not changed.

The different sets of implementation criteria are consolidated into one set of criteria under § 164.508(c), thus eliminating the confusion and uncertainty associated with different requirements for specific circumstances. Covered entities may use one authorization form for all purposes. The Department adopts in paragraph (c)(1), the following core elements for a valid authorization: (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. An authorization that does not contain all of the core elements does not meet the requirements for a valid authorization. The Department intends for the authorization process to provide individuals with the opportunity to know and understand the circumstances surrounding a requested authorization.

To further protect the privacy interests of individuals, when individuals initiate an authorization for their own purposes, the purpose may be stated as ''at the request of the individual.'' Other changes to the core elements pertain to authorizations for research, and are discussed in section III.E.2. of the preamble.

Also, under § 164.508(c)(2), an authorization is not valid unless it contains all of the following: (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, 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 redisclosed by the recipient. Although the notification statements are not included in the paragraph on core elements an authorization is not valid unless it contains both the required core elements, and all of the required statements. This is the minimum information the Department believes is needed to ensure individuals are fully informed of their rights with respect to an authorization and to understand the consequences of authorizing the use or disclosure. The required statements must be written in a manner that is adequate to place the individual on notice of the substance of the statements.

In response to comments, the Department clarifies that the statement regarding the potential for redisclosure does not require an analysis of the risk for redisclosure, but may be a general statement that the health information may no longer be protected by the Privacy Rule once it is disclosed by the covered entity. Others objected to this statement because individuals might be hesitant to sign an authorization if they knew their protected health information could be redisclosed and no longer protected by the Rule. In response, the Department believes that individuals need to know about the consequences of authorizing the disclosure of their protected health information. As the commenter recognized, the potential for redisclosure may, indeed, be an important factor in an individual's decision to give or deny a requested authorization.

Others suggested that the statement regarding redisclosure should be omitted when an authorization is obtained only for a use, since such a statement would be confusing and

inappropriate when the covered entity maintains the information. Similarly, some commenters were concerned that the statement may be misleading where the recipient of the information, although not a covered entity, will keep the information confidential. In response, the Department clarifies that, while a general statement would suffice, a covered entity has the discretion to provide a more definitive statement where appropriate. Thus, the covered entity requesting an authorization for its own use of protected health information may provide assurances that the information will remain subject to the Privacy Rule. Similarly, if a third party, such as a researcher, is seeking an authorization for research, the statement may refer to the privacy protections that the researcher will provide for the data.

Under § 164.508(c)(3), authorizations must be written in plain language so that individuals can understand the information contained in the form, and thus be able to make an informed decision about whether to give the authorization. A few commenters urged the Department to keep the plain language requirement as a core element of a valid authorization. Under the December 2000 Rule, the plain language requirement was not a requisite for a valid authorization. Nevertheless, under both the December 2000 Rule and the final modifications, authorizations must be written in plain language. The fact that the plain language requirement is not a core element does not diminish its importance or effect, and the failure to meet this requirement is a violation of the Rule.

Finally, under § 164.508(c)(4), covered entities who seek an authorization are required to provide the individual with a copy of the signed authorization form.

Response to Other Public Comments

Comment: A number of commenters specifically expressed support of the proposed authorization requirement for marketing, and urged the Department to adopt the requirement. However, one commenter claimed that requiring authorizations for marketing would reduce hospitals' ability to market their programs and services effectively in order to compete in the marketplace, and that obtaining, storing, and maintaining marketing authorizations would be too burdensome.

Response: In light of the support in the comments, the Department has adopted the proposed requirement for an authorization before a covered entity may use or disclose protected health information for marketing. However, the commenter is mistaken that this requirement will interfere with a hospital's ability to promote its own program and services within the community. First, such broad-based marketing is likely taking place without resort to protected health information, through dissemination of information about the hospital through community-wide mailing lists. Second, under the Privacy Rule, a communication is not marketing if a covered entity is describing its own products and services. Therefore, nothing in the Rule will inhibit a hospital from competing in the marketplace by communicating about its programs and services.

Comment: One commenter suggested that authorizations for marketing should clearly indicate that they are comprehensive and may contain sensitive protected health information.

Response: The Department treats all individually identifiable health information as sensitive and equally deserving of protections under the Privacy Rule. The Rule requires all authorizations to contain the specified core elements to ensure individuals are given the information they need to make an informed decision. One of the core elements for all authorizations is a clear description of the information that is authorized to be used or disclosed in specific and meaningful terms. The authorization process provides the individual with the opportunity to ask questions, negotiate how their information will be used and disclosed, and ultimately to control whether these uses and disclosures will be made.

Comment: Several commenters urged the Department to retain the existing structure of the implementation specifications, whereby the notification statements about the individual's right to revoke and the potential for redisclosure are ''core elements.'' It was argued that this information is essential to an informed decision. One of the commenters claimed that moving them out of the core elements and only requiring a statement adequate to put the person on notice of the information would increase uncertainty, and that these two elements are too important to risk inadequate explanation.

Response: The Department agrees that the required notification statements are essential information that a person needs in order to make an informed decision about authorizing the use or disclosure of protected health information. Individuals need to know what rights they have with respect to an authorization, and how they can exercise those rights. However, separating the core elements and notification statements into two different subparagraphs does not diminish the importance or effect of the notification statements. The Department clarifies that both the core elements and the notification statements are required, and both must be included for an authorization to be valid.

Comment: Several commenters urged the Department to eliminate unnecessary authorization contents. They argued the test should be whether the person needs the information to protect his or her privacy, and cited the disclosure of remuneration by a third party as an example of unnecessary content, alleging that the disclosure of remuneration is not relevant to protecting privacy. One commenter suggested that covered entities should be given the flexibility to decide which contents are applicable in a given situation.

Response: The Department believes the core elements are all essential information. Individuals need to know this information to make an informed decision about giving the authorization to use or disclose their protected health information. Therefore, the Department believes all of the core elements are necessary content in all situations. The Department does not agree that the remuneration statement required on an authorization for uses and disclosures of an individual's protected health information for marketing purposes is not relevant to protecting privacy. Individuals exercise control over the privacy of their protected health information by either giving or denying an authorization, and remuneration from a third party to the covered entity for obtaining an authorization for marketing is an important factor in making that choice.

Comment: One commenter suggested that covered entities should not be required to state on an authorization a person's authority to act on an individual's behalf, and they should be trusted to require such identification or proof of legal authority when the authorization is signed. The commenter stated that this requirement only increases administrative burden for covered entities.

Response: The Department does not agree. The authorization requirement is intended to give individuals some control over uses and disclosures of protected health information that are not otherwise permitted or required by the Rule. Therefore, the Rule requires that covered entities verify and document a person's authority to sign an authorization on an individual's behalf, since that person is exercising the individual's control of the information. Furthermore, the Department understands that it is a

current industry standard to verify and document a person's authority to sign any legal permission on another person's behalf. Thus, the requirement should not result in any undue administrative burden for covered entities.

Comment: One commenter suggested that the Department should require authorizations to include a complete list of entities that will use and share the information, and that the individual should be notified periodically of any changes to the list so that the individual can provide written authorization for the changes.

Response: It may not always be feasible or practical for covered entities to include a comprehensive list of persons authorized to use and share the information disclosed pursuant to an authorization. However, individuals may discuss this option with covered entities, and they may refuse to sign an authorization that does not meet their expectations. Also, subject to certain limitations, individuals may revoke an authorization at any time.

Comment: One commenter asked for clarification that a health plan may not condition a provider's participation in the health plan on seeking authorization for the disclosure of psychotherapy notes, arguing that this practice would coerce providers to request, and patients to provide, an authorization to disclose psychotherapy notes.

Response: The Privacy Rule does not permit a health plan to condition enrollment, eligibility for benefits, or payment of a claim on obtaining the individual's authorization to use or disclose psychotherapy notes. Nor may a health care provider condition treatment on an authorization for the use or disclosure of psychotherapy notes. In a situation such as the one described by the commenter, the Department would look closely at whether the health plan was attempting to accomplish indirectly that which the Rule prohibits. These prohibitions are to ensure that the individual's permission is wholly voluntary and informed with regard to such an authorization. To meet these standards, in the circumstances set forth in the comment, the Department would expect the provider subject to such a requirement by the health plan to explain to the individual in very clear terms that, while the provider is required to ask, the individual remains free to refuse to authorize the disclosure and that such refusal will have no effect on either the provision of treatment or the individual's coverage under, and payment of claims by, the health plan.

Comment: A few commenters suggested the Department should allow covered entities to combine an authorization with other documents, such as the notice acknowledgment, claiming it would reduce administrative burden and paperwork, as well as reduce patient confusion and waiting times, without compromising privacy protections.

Response: The Department disagrees that combining an authorization with other documents, such as the notice acknowledgment, would be less confusing for individuals. To the contrary, the Department believes that combining unrelated documents would be more confusing. However, the Rule does permit an authorization to be combined with other authorizations so long as the provision of treatment, payment, enrollment in a health plan or eligibility for benefits is not conditioned on obtaining any of the authorizations, and the authorization is not for the use or disclosure of psychotherapy notes.

Also, authorizations must contain the same information, whether it is a separate document or combined with another document; and the individual must be given the opportunity to read and discuss that information. Combining an authorization with routine paperwork diminishes individuals' ability to make a considered and informed judgment to permit the use or disclosure of their medical information for some other purpose.

Comment: One commenter stated that the requirement for covered entities to use only authorizations that are valid under the Rule must be an unintended result of the Rule, because covered entities would have to use only valid authorizations when requesting information from non-covered entities. The commenter did not believe the Department intended this requirement to apply with respect to non-covered entities, and gave the example of dental health plans obtaining protected health information in connection with paper claims submitted by dental offices. The commenter requested clarification that health plans may continue to use authorization forms currently in use for all claims submitted by non-covered entities.

Response: The commenter misapprehends the Rule's requirements. The requirements apply to uses and disclosure of protected health information by covered entities. In the example provided, where a health plan is requesting additional information in support of a claim for payment by a non-covered health care provider, the health plan is not required to use an authorization. The plan does not need the individual's authorization to use protected health information for payment purposes, and the non-covered health care provider is not subject to any of the Rule's requirements. Therefore, the exchange of information may occur as it does today. The Department notes that, based on the modifications regarding consent adopted in this rulemaking, neither a consent nor an authorization would be required in this example even if the health care provider was also a covered entity.

Comment: Several commenters urged the Department to add a transition provision to permit hospitals to use protected health information in already existing databases for marketing and outreach to the communities they serve. Commenters claimed that these databases are important assets that would take many years to rebuild, and hospitals may not have an already existing authorization or other express legal permission for such use of the information. They contended that, without a transition provision, these databases would become useless under the Rule. Commenters suggested the Department should adopt an ''opt out'' provision that would allow continued use of these databases to initially communicate with the persons listed in the database; at that time, they could obtain authorization for future communications, thus providing a smooth transition.

Response: Covered entities are provided a two-year period in which to come into compliance with the Privacy Rule. One of the purposes of the compliance period is to allow covered entities sufficient time to undertake actions such as those described in the comment (obtaining the legal permissions that would permit databases to continue to operate after the compliance date). An additional transition period for these activities has not been justified by the commenters. However, the Department notes that a covered entity is permitted to use the information in a database for communications that are either excepted from or that do not meet the definition of ''marketing'' in § 164.501, without individual authorization. For example, a hospital may use protected health information in an existing database to distribute information about the services it provides, or to distribute a newsletter with general health or wellness information that does not promote a particular product or service.

2. Research Authorizations

December 2000 Privacy Rule. The Privacy Rule requires covered entities to 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 Rule. Uses and disclosures of protected health information for research purposes are subject to the same authorization requirements as uses and disclosures for other purposes. However, for research that includes treatment of the individual, the December 2000 Privacy Rule prescribed special authorization requirements at § 164.508(f). The December 2000 Privacy Rule, at § 164.508(b)(5), also permitted individuals to revoke their authorization at any time, with limited exceptions. Further, the December 2000 Privacy Rule prohibited the combining of the authorization for the use or disclosure of existing protected health information with any other legal permission related to the research study.

March 2002 NPRM. Several of those who commented on the December 2000 Privacy Rule argued that certain authorization requirements in § 164.508 were unduly complex and burdensome as applied to research uses and disclosures. In particular, several commenters favored eliminating the Rule's specific provisions at § 164.508(f) for authorizations for uses and disclosures of protected health information for research that includes treatment of the individual. The Department also heard from several provider groups who 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 the research. Commenters also noted that the Rule's requirement for an ''expiration date or event that relates to the individual or the purpose of the use or disclosure'' runs counter to the needs of research databases and repositories that are often retained indefinitely.

In response to these concerns, the Department proposed to a number of modifications to simplify the authorization requirements both generally, and in certain circumstances, as they specifically applied to uses and disclosures of protected health information for research. In particular, the Department proposed a single set of authorization requirements for all uses and disclosures, including those for research purposes. This proposal would eliminate the additional authorization requirements for the use and disclosure of protected health information created for research that includes treatment of the individual. Consistent with this proposed change, the Department further proposed to modify the requirements prohibiting the conditioning of authorizations at § 164.508(b)(4)(i) to remove the reference to § 164.508(f).

In addition, the Department proposed that the Privacy Rule permit an authorization for the use or disclosure of protected health information to be combined with any other legal permission related to the research study, including another authorization or consent to participate in the research.

Finally, the Department proposed to provide explicitly that the statement, ''end of a research study,'' or similar language be sufficient to meet the requirement for an expiration date in § 164.508(c)(1)(v). Additionally, the Department proposed that the statement ''none'' or similar language be sufficient to meet this provision if the authorization was for a covered entity to use or disclose protected health information for the creation or maintenance of a research database or repository.

Overview of Public Comments. The following discussion provides an overview of the public comment received on this proposal. Additional comments received on this issue are discussed below in the section entitled, ''Response to Other Public Comments.''

The vast majority of commenters were very supportive of the proposed revisions to the Rule's provisions for research authorizations. However, the Department did hear from several commenters that the Privacy Rule's requirement for an expiration date or event should be eliminated for all research uses and disclosures of protected health information, not just for uses and disclosures for the creation or maintenance of a research database or repository, as was proposed in the NPRM. These commenters were concerned that the Privacy Rule would prohibit important uses and disclosures of protected health information after the termination of a research project, such as the reporting of research results to the Food and Drug Administration (FDA) for an FDA investigational new drug application, unless the covered entity obtained another patient authorization. In addition, several of these commenters cited confusion in defining repositories and databases. Some of these commenters stated that an individual who authorizes information to be used for an indeterminate time most likely expects and intends for the information to be used and disclosed if needed well into the future, regardless of whether or not the research involves the use or disclosure of protected health information for the creation or maintenance of a database or repository.

Several commenters responded to the Department's request for comments on how to appropriately limit uses and disclosures following revocation of an authorization, while preserving the integrity of the research. The NPRM attempted to clarify that ''even though a revocation will prevent 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 information as appropriate to preserve the integrity of the research study.'' However, the NPRM further stated that ''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.'' Several commenters were concerned and confused by the NPRM's statements. In particular, the Department received comments urging that the regulation permit covered entities to use and disclose research data already obtained, even after an individual has withdrawn his or her authorization. These commenters suggested that once a subject has authorized the use and disclosure of protected health information for research and the covered entity has relied on the authorization, the covered entity must retain the ability to use or disclose the subject's pre-withdrawal information for purposes consistent with the overall research. One commenter argued that it would be inadequate for the reliance exception at § 164.508(b)(5) to be interpreted to permit continued uses of the individual's information as appropriate only to account for an individual's withdrawal from the study. In this commenter's opinion, most research would call for the continued use of protected health information obtained prior to an individual's revocation of their authorization to safeguard statistical validity and truly to preserve the integrity of human research.

Final Modifications. The Department agrees with the commenters that supported the NPRM's proposed simplification of authorizations for research uses and disclosures of protected health information and, therefore, adopts the modifications to these provisions as proposed in the NPRM. The final Rule requires a single

set of authorization requirements for all uses and disclosures, including those for research purposes, and permits an authorization for the use or disclosure of protected health information to be combined with any other legal permission related to the research study, including another authorization or consent to participate in the research.

In addition, in response to commenters' concerns that the Rule would prohibit important uses and disclosures of protected health information after the termination of a research project, the final Rule eliminates the requirement for an expiration date for all uses and disclosures of protected health information for research purposes, not only for the creation and maintenance of a research database or repository. The Department agrees that the line between research repositories and databases in particular, and research data collection in general, is sometimes arbitrary and unclear. If the authorization for research uses and disclosures of protected health information does not have an expiration date, the final Rule at § 164.508(c)(1)(v), requires that this fact be stated on the authorization form. Patients continue to control whether protected health information about them may be used or disclosed for research, since the authorization must include an expiration date or event, or a statement that the authorization will have no expiration date. In addition, patients will be permitted to revoke their authorization at any time during the research project, except as specified under § 164.508(b)(5). However, the Department notes that researchers may choose to include, and covered entities may choose to require, an expiration date when appropriate.

Although the final Rule does not modify the revocation provision at § 164.508(b)(5), in response to commenters' concerns, the Department clarifies that this provision permits covered entities to continue using and disclosing protected health information that was obtained prior to the time the individual revoked his or her authorization, as necessary to maintain the integrity of the research study. An individual may not revoke an authorization to the extent the covered entity has acted in reliance on the authorization. For research uses and disclosures, this reliance exception at § 164.508(b)(5)(i) permits the continued use and disclosure of protected health information already obtained pursuant to a valid authorization to the extent necessary to preserve the integrity of the research study. For example, the reliance exception would permit the continued use and disclosure of protected health information to account for a subject's withdrawal from the research study, as necessary to incorporate the information as part of a marketing application submitted to the FDA, to conduct investigations of scientific misconduct, or to report adverse events. However, the reliance exception would not permit a covered entity to continue disclosing additional protected health information to a researcher or to use for its own research purposes information not already gathered at the time an individual withdraws his or her authorization. The Department believes that this clarification of the Rule will minimize the negative effects on research caused by participant withdrawal and will allow for important continued uses and disclosures to occur, while maintaining privacy protections for research subjects.

Response to Other Public Comments

Comment: In opposition to the March 2002 NPRM, one commenter suggested prohibiting the combining of authorization forms with an informed consent when the covered entity disclosing the protected health information is not otherwise participating in research. The commenter argued that the NPRM would allow covered entities to receive more information than necessary to fulfill a patient's authorization request, such as information about the particular type or purpose of the study itself, and could, thereby, violate the patient's privacy.

Response: The Department acknowledges the concern raised by these commenters; however, prohibiting the combination of authorization forms with an informed consent reduces the flexibility proposed in the March 2002 NPRM. Since the final modifications permit—but do not require—such combining of forms, the Department has decided to leave it to the discretion of researchers or the IRBs to determine whether the combining of authorization forms and consent forms for research would be appropriate for a particular research study.

Comment: Some commenters supported retaining the December 2000 Privacy Rule requirement that a description of the extent to which protected health information will be used or disclosed for treatment, payment, or health care operations be included in an authorization to use or disclose protected health information for a research study that includes treatment of individuals. These commenters argued that an individual's ability to make informed decisions requires that he or she know how research information will and will not be used and disclosed.

Response: The Department agrees with the majority of the commenters who were in support of the March 2002 NPRM proposal to eliminate the additional authorization requirements for research that includes treatment, and has adopted these proposed modifications in the final Rule. Retaining the distinction between research that involves treatment and research that does not would require overly subjective decisions without providing commensurate privacy protections for individuals. However, the Department notes that it may sometimes be advisable for authorization forms to include a statement regarding how protected health information obtained for a research study will be used and disclosed for treatment, payment, and health care operations, if such information would assist individuals in making informed decisions about whether or not to provide their authorization for a research study.

Comment: One commenter argued that expiration dates should be included on authorizations and that extensions should be required for all research uses and disclosures made after the expiration date or event has passed.

Response: The Department disagrees. We have determined that an expiration date or event would not always be feasible or desirable for some research uses and disclosures of protected health information. By allowing for no expiration date, the final Rule permits without separate patient authorization important disclosures even after the ''termination of the research project'' that might otherwise be prohibited. However, the final Rule contains the requirement that the patient authorization specify if the authorization would not have an expiration date or event. Therefore, patients will have this information to make an informed decision about whether to sign the authorization.

Comment: Another commenter suggested permitting covered entities/researchers to continue using or disclosing protected health information even after a revocation of the initial authorization but only if an IRB or Privacy Board approved the continuation. This commenter argued that such review by an IRB or Privacy Board would protect privacy, while permitting continued uses and disclosures of protected health information for important purposes.

Response: As stated above, the Department agrees that it may sometimes be necessary to continue using and disclosing protected health information even after an individual has revoked his or her authorization in order to preserve the integrity of a research study. Therefore, the Department has clarified that the reliance exception at § 164.508(b)(5)(i) would permit the continued use and disclosure of protected health information already obtained pursuant to a valid authorization to the extent necessary to preserve the integrity of the research study. A requirement for documentation of IRB or Privacy Board review and approval of the continued use or disclosure of protected health information after an individual's authorization had been revoked could protect patient privacy. However, the Department believes that the additional burden on the IRB or Privacy Board could be substantial, and is not warranted at this time.

Comment: A commenter requested clarification that the ''reliance exception'' does not permit covered entities as researchers to continue analyzing data once an individual has revoked his or her authorization.

Response: As discussed above, the Department disagrees with this comment. Patient privacy must be balanced against other public goods, such as research and the risk of compromising such research projects if researchers could not continue to use such data. The Department determined that permitting continued uses and disclosures of protected health information already obtained to protect the integrity of research, even after an individual's authorization has been revoked, would pose minimal privacy risk to individuals without compromising research.

Comment: Several commenters suggested permitting the proposed authorization requirement for a ''description of each purpose of the requested use or disclosure'' at § 164.508 to be sufficiently broad to encompass future unspecified research. These commenters argued that this option would reduce the burden for covered entities and researchers by permitting covered entities to use or disclose protected health information for re-analysis without having to obtain an additional authorization from the individual. Some discussed the possibility that burden for patients would also be reduced because they would not have to provide additional authorizations. These commenters also argued that such a provision would more directly align the Rule with the Common Rule, which permits broad informed consent for secondary studies if the IRB deems the original informed consent to be adequate.

Response: The Department disagrees with broadening the required ''description of the purpose of the use or disclosure'' because of the concern that patients would lack necessary information to make an informed decision. In addition, unlike the Common Rule, the Privacy Rule does not require IRB or Privacy Board review of research uses and disclosures made with individual authorization. Therefore, instead of IRBs or Privacy Boards reviewing the adequacy of existing patient authorizations, covered entities would be left to decide whether or not the initial authorization was broad enough to cover subsequent research analyses. Furthermore, it should be noted that patient authorization would not be required for such re-analysis if, with respect to the re-analysis, the covered entity obtains IRB or Privacy Board waiver of such authorization as required by § 164.512(i). For these reasons, the Department has decided to retain the requirement that each purpose of the requested use or disclosure described in the authorization form be research study specific. However, the Department understands that, in the past, some express legal permissions and informed consents have not been study-specific and sometimes authorize the use or disclosure of information for future unspecified research. Furthermore, some IRB-approved waivers of informed consent have been for future unspecified research. Therefore, the final Rule at § 164.532 permits covered entities to rely on an express legal permission, informed consent, or IRB-approved waiver of informed consent for future unspecified research, provided the legal permission, informed consent or IRB-approved waiver was obtained prior to the compliance date.

Comment: Several commenters suggested retaining the authorization element requiring a statement regarding ''the potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer protected by this Rule'' but with one addition. This addition would state that ''researchers could only use or disclose the protected health information for purposes approved by the IRB or as required by law or regulation.'' These commenters argued that this would be clearer to participants and would prevent the misconception that their information would not be protected by any confidentiality standards.

Response: The Department recognizes the concern of the commenters seeking to supplement the requirement, but points out that, although the final Rule will not require this addition, it is permissible to include such a statement in the authorization. In addition, since the Privacy Rule does not require IRB or Privacy Board review of research uses and disclosures made with patient authorization, the Department determined that adding the commenters' suggestion to the final Rule would be inappropriate. Section III.E.1. above provides further discussion of this provision.

F. Section 164.512—Uses and Disclosures for Which Authorization or Opportunity To Agree or Object Is Not Required

1. Uses and Disclosures Regarding FDA-Regulated Products and Activities

December 2000 Privacy Rule. The Privacy Rule permits covered entities to disclose protected health information without consent or authorization for public health purposes. Generally, these disclosures may be made to public health authorities, as well as to contractors and agents of public health authorities. However, in recognition of the essential role of drug and medical device manufacturers and other private persons in carrying out the Food and Drug Administration's (FDA) public health mission, the December 2000 Privacy Rule permitted covered entities to make such disclosures to a person who is subject to the jurisdiction of the FDA, but only 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.

March 2002 NPRM. The Department heard a number of concerns about the scope of the disclosures permitted for FDA-regulated products and activities and the failure of the Privacy Rule to reflect the breadth of the public health activities currently conducted by private sector entities subject to the jurisdiction of the FDA on a voluntary basis. These commenters claimed the Rule would constrain important public health surveillance and reporting activities by

impeding the flow of needed information to those subject to the jurisdiction of the FDA. For instance, there were concerns that the Rule would have a chilling effect on current voluntary reporting practices. The FDA gets the vast majority of information concerning problems with FDA-regulated products, including drugs, medical devices, biological products, and food indirectly through voluntary reports made by health care providers to the manufacturers. These reports are critically important to public health and safety. The December 2000 Rule permitted such disclosures only when made to a person ''required or directed'' to report the information to the FDA or to track the product. The manufacturer may or may not be required to report such problems to the FDA, and the covered entities who make these reports are not in a position to know whether the recipient of the information is so obligated. Consequently, many feared that this uncertainty would cause covered entities to discontinue their practices of voluntary reporting of adverse events related to FDA-regulated products or entities.

Some covered entities also expressed fears of the risk of liability should they inadvertently report the information to a person who is not subject to the jurisdiction of the FDA or to the wrong manufacturer. Hence, they urged the Department to provide a ''good-faith'' safe harbor to protect covered entities from enforcement actions arising from unintentional violations of the Privacy Rule.

A number of commenters, including some subject to the jurisdiction of the FDA, suggested that it is not necessary to disclose identifiable health information for some or all of these public health purposes, that identifiable health information is not reported to the FDA, and that information without direct identifiers (such as name, mailing address, phone number, social security number, and email address) is sufficient for post-marketing surveillance purposes.

The Rule is not intended to discourage or prevent adverse event reporting or otherwise disrupt the flow of essential information that the FDA and persons subject to the jurisdiction of the FDA need in order to carry out their important public health activities. Therefore, the Department proposed some modifications to the Rule to address these issues in the NPRM. Specifically, the Department proposed 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, the Department proposed to describe at the outset the public health purposes for which disclosures may be made. The proposed language read: ''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 proposal retained the specific activities identified in paragraphs (A), (B), (C), and (D) as examples of common FDA purposes for which disclosures would be permitted, but eliminated the language that would have made this listing the only activities for which such disclosures would be allowed. These activities include reporting of adverse events and other product defects, the tracking of FDA-regulated products, enabling product recalls, repairs, or replacement, and conducting post-marketing surveillance. Additionally, the Department proposed to include ''lookback'' activities in paragraph (C), which are necessary for tracking blood and plasma products, as well as quarantining tainted blood or plasma and notifying recipients of such tainted products.

In addition to these specific changes, the Department solicited comments on whether a 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 also requested comments as to whether the proposed modifications would be sufficient, or if additional measures, such as a good-faith safe harbor, would be needed for covered entities to continue to report vital information concerning FDA-regulated products or activities on a voluntary basis.

Overview of Public Comments. The following discussion provides an overview of the public comment received on this proposal. Additional comments received on this issue are discussed below in the section entitled, ''Response to Other Public Comments.''

The proposed changes received wide support. The overwhelming majority of commenters urged the Department to adopt the proposed changes, claiming it would reduce the chilling effect that the Rule would otherwise have on current voluntary reporting practices, which are an important means of identifying adverse events, defects, and other problems regarding FDA-regulated products. Several commenters further urged the Department to provide a good-faith safe harbor to allay providers' fears of inadvertently violating the Rule, stating that covered entities would otherwise be reluctant to risk liability to make these important public health disclosures.

A few commenters opposed the proposed changes, expressing concern that the scope of the proposal was too broad. They were particularly concerned that including activities related to ''quality'' or ''effectiveness'' would create a loophole for manufacturers to obtain and use protected health information for purposes the average person would consider unrelated to public health or safety, such as using information to market products to individuals. Some of these commenters said the Department should retain the exclusive list of purposes and activities for which such disclosures may be made, and some urged the Department to retain the ''required or directed'' language, as it creates an essential nexus to a government authority or requirement. It was also suggested that the chilling effect on reporting of adverse events could be counteracted by a more targeted approach. Commenters were also concerned that the proposal would permit disclosure of much more protected health information to non-covered entities that are not obligated by the Rule to protect the privacy of the information. Comments regarding use of a limited data set for public health disclosures are discussed in section III.G.1. of the preamble.

Final Modifications. In the final modifications, the Department adopts the language proposed in the NPRM. Section 164.512(b)(1)(iii), as modified, permits covered entities to disclose protected health information, without authorization, to a person subject to the jurisdiction of the 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, but are not limited to, the following activities and purposes listed in subparagraphs (A) through (D): (1) To collect or report adverse events (or similar activities regarding food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations, (2) to track FDA-regulated products, (3) to enable product recalls, repairs, or replacement, or for lookback (including locating and notifying persons who have

received products that have been withdrawn, recalled, or are the subject of lookback), and (4) to conduct post-marketing surveillance.

The Department believes these modifications are necessary to remove barriers that could prevent or chill the continued flow of vital information between health care providers and manufacturers of food, drugs, medical and other devices, and biological products. Health care providers have been making these disclosures to manufacturers for many years, and commenters opposed to the proposal did not cite any examples of abuses of information disclosed for such purposes. Furthermore, both the individuals who are the subjects of the information and the general public benefit from these disclosures, which are an important means of identifying and dealing with FDA-regulated products on the market that potentially pose a health or safety threat. For example, FDA learns a great deal about the safety of a drug after it is marketed as a result of voluntary adverse event reports made by covered entities to the product's manufacturer. The manufacturer is required to submit these safety reports to FDA, which uses the information to help make the product safer by, among other things, adding warnings or changing the product's directions for use. The modifications provide the necessary assurances to covered entities that such voluntary reporting may continue.

Although the list of permissible disclosures is no longer exclusive, the Department disagrees with commenters that asserted the modifications permit virtually unlimited disclosures for FDA purposes. As modified, such disclosures must still be made to a person subject to the jurisdiction of the FDA. The disclosure also must relate to FDA-regulated products or activities for which the person using or receiving the information has responsibility, and be made only for activities related to the safety, effectiveness, or quality of such FDA-regulated product or activity. These terms are terms of art with commonly accepted and understood meanings in the FDA context, meanings of which providers making such reports are aware. This limits the possibility that FDA-regulated manufacturers and entities will able to abuse this provision to obtain information to which they would otherwise not be entitled.

Moreover, § 164.512(b)(1) specifically limits permissible disclosures to those made for public health activities and purposes. While a disclosure related to the safety, quality or effectiveness of an FDA-regulated product is a permissible disclosure, the disclosure also must be for a ''public health'' activity or purpose. For example, it is not permissible under § 164.512(b)(1)(iii) for a covered entity to disclose protected health information to a manufacturer to allow the manufacturer to evaluate the effectiveness of a marketing campaign for a prescription drug. In this example, although the disclosure may be related to the effectiveness of an FDA-regulated activity (the advertising of a prescription drug), the disclosure is made for the commercial purposes of the manufacturer rather than for a public health purpose.

A disclosure related to a ''quality'' defect of an FDA-regulated product is also permitted. For instance, the public health exception permits a covered entity to contact the manufacturer of a product to report drug packaging quality defects. However, this section does not permit all possible reports from a covered entity to a person subject to FDA jurisdiction about product quality. It would not be permissible for a provider to furnish a manufacturer with a list of patients who prefer a different flavored cough syrup over the flavor of the manufacturer's product. Such a disclosure generally would not be for a public health purpose. However, a disclosure related to the flavor of a product would be permitted under this section if the covered entity believed that a difference in the product's flavor indicated, for example, a possible manufacturing problem or suggested that the product had been tampered with in a way that could affect the product's safety.

The Department clarifies that the types of disclosures that covered entities are permitted to make to persons subject to FDA jurisdiction are those of the type that have been traditionally made over the years. These reports include, but are not limited to, those made for the purposes identified in paragraphs (A)–(D) of § 164.512(b)(1)(iii) of this final Rule.

Also, the minimum necessary standard applies to public health disclosures, including those made to persons subject to the jurisdiction of the FDA. There are many instances where a report about the quality, safety, or effectiveness of an FDA-regulated product can be made without disclosing protected health information. Such may be the case with many adverse drug events where it is important to know what happened but it may not be important to know to whom. However, in other circumstances, such as device tracking or blood lookback, it is essential for the manufacturer to have identifying patient information in order to carry out its responsibilities under the Food, Drug, and Cosmetic Act. Therefore, identifiable health information can be disclosed for these purposes, consistent with the minimum necessary standard.

As the Department stated in the preamble of the NPRM, ''a person'' subject to the jurisdiction of the FDA does not mean that the disclosure must be made to a specific individual. The Food, Drug, and Cosmetic Act defines ''person'' to include an individual, partnership, corporation, and association. Therefore, covered entities may continue to disclose protected health information to the companies subject to FDA's jurisdiction that have responsibility for the product or activity. Covered entities may identify responsible companies by using information obtained from product labels or product labeling (written material about the product that accompanies the product) including sources of labeling, such as the Physician's Desk Reference.

The Department believes these modifications effectively balance the privacy interests of individuals with the interests of public health and safety. Since the vast majority of commenters were silent on the question of the potential need for a ''good faith'' exception, the Department believes that these modifications will be sufficient to preserve the current public health activities of persons subject to the jurisdiction of the FDA, without such a safe harbor. However, the Department will continue to evaluate the effect of the Rule to determine whether there is need for further modifications or guidance.

Response to Other Public Comments

Comment: A few commenters urged the Department to include foreign public health authorities in the Rule's definition of ''public health authority.'' These commenters claimed that medical products are often distributed in multiple countries, and the associated public health issues are experienced globally. They further claimed that requiring covered entities to obtain the permission of a United States-based public health authority before disclosing protected health information to a foreign government public health authority will impede important communications.

Response: The Department notes that covered entities are permitted to disclose protected health information for public health purposes, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority. The

Department does not have sufficient information at this time as to any potential impacts or workability issues that could arise from this language and, therefore, does not modify the Rule in this regard.

Comment: Some commenters, who opposed the proposal as a weakening of the Privacy Rule, suggested that the Department implement a more targeted approach to address only those issues raised in the preamble to the NPRM, such as voluntary adverse event reporting activities, rather than broadening the provision generally.

Response: The NPRM was intended to address a number of issues in addition to the concern that the December 2000 Privacy Rule would chill reporting of adverse events to entities from whom the FDA receives much of its adverse event information. For instance, the text of the December 2000 Privacy Rule did not expressly permit disclosure of protected health information to FDA-regulated entities for the purpose of enabling ''lookback,'' which is an activity performed by the blood and plasma industry to identify and quarantine blood and blood products that may be at increased risk of transmitting certain blood-borne diseases, and which includes the notification of individuals who received possibly tainted products, permitting them to seek medical attention and counseling. The NPRM also was intended to simplify the public health reporting provision and to make it more readily understandable. Finally, the approach proposed in the NPRM, and adopted in this final Rule, is intended to add flexibility to the public health reporting provision of the December 2000 Rule, whose exclusive list of permissible disclosures was insufficiently flexible to assure that § 164.512(b)(1)(iii) will allow legitimate public health reporting activities that might arise in the future.

In addition, the Department clarifies that the reporting of adverse events is not restricted to the FDA or persons subject to the jurisdiction of the FDA. A covered entity may, under § 164.512(b), disclose protected health information to a public health authority that is authorized to receive or collect a report on an adverse event. In addition, to the extent an adverse event is required to be reported by law, the disclosure of protected health information for this purpose is also permitted under § 164.512(a). For example, a Federally funded researcher who is a covered health care provider under the Privacy Rule may disclose protected health information related to an adverse event to the National Institutes of Health (NIH) if required to do so by NIH regulations. Even if not required to do so, the researcher may also disclose adverse events directly to NIH as a public health authority. To the extent that NIH has public health matters as part of its official mandate it qualifies as a public health authority under the Privacy Rule, and to the extent it is authorized by law to collect or receive reports about injury and other adverse events such collection would qualify as a public health activity.

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

December 2000 Privacy Rule. The Privacy Rule builds upon existing Federal regulations governing the conduct of human subjects research. In particular, the Rule at § 164.512(i) establishes conditions under which covered entities can use and disclose protected health information for research purposes without individual authorization if the covered entity first obtains either of the following:

- Documentation of approval of a waiver of authorization from an Institutional Review Board (IRB) or a Privacy Board. The Privacy Rule specifies requirements that must be documented, including the Board's determination that eight defined waiver criteria had been met.
- Where a review of protected health information is conducted preparatory to research or where research is conducted solely on decedents' 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.

March 2002 NPRM. A number of commenters informed the Department that the eight waiver criteria in the December 2000 Privacy Rule were confusing, redundant, and internally inconsistent. These commenters urged the Department to simplify these provisions, noting that they would be especially burdensome and duplicative for research that was currently governed by the Common Rule. In response to these comments, the Department proposed the following modifications to the waiver criteria for all research uses and disclosures of protected health information, regardless of whether or not the research is subject to the Common Rule:

- The Department proposed to delete the criterion that ''the alteration or waiver will not adversely affect the privacy rights and the welfare of the individuals,'' because it may conflict with the criterion regarding the assessment of minimal privacy risk.
- In response to commenters' concerns about the overlap and potential inconsistency among several of the Privacy Rule's criteria, the Department proposed to turn the following three criteria into factors that must be considered as part of the IRB's or Privacy Board's assessment of minimal risk to privacy:
- There is an adequate plan to protect the identifiers from improper use and disclosure;
- There is an adequate plan to destroy the identifiers at the earliest opportunity consistent with the conduct of the research, unless there is a health or research justification for retaining the identifiers, or such retention is otherwise required by law; and
- There are adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of protected health information would be permitted by this subpart.
- In response to concerns that the following waiver criterion was unnecessarily duplicative of other provisions to protect patients' confidentiality interests, the Department proposed to eliminate the criterion that: ''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.''

In sum, the NPRM proposed that the following waiver criteria replace the waiver criteria in the December 2000 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.

Overview of Public Comments. The following discussion provides an overview of the public comment received on this proposal. Additional comments received on this issue are discussed below in the section entitled, ''Response to Other Public Comments.''

The overwhelming majority of commenters were supportive of the Department's proposed modifications to the Privacy Rule's waiver criteria. These commenters found that the proposed revisions adequately addressed earlier concerns that the waiver criteria in the December 2000 Rule were confusing, redundant, and internally inconsistent. However, a few commenters argued that some of the proposed criteria continued to be too subjective and urged that they be eliminated.

Final Modifications. The Department agrees with the majority of commenters that supported the proposed waiver criteria, and adopts the modifications as proposed in the NPRM. The criteria safeguard patient privacy, require attention to issues sometimes currently overlooked by IRBs, and are compatible with the Common Rule. Though IRBs and Privacy Boards may initially struggle to interpret the criteria, as a few commenters mentioned, the Department intends to issue guidance documents to address this concern. Furthermore, the Department notes that experience and guidance have enabled IRBs to successfully implement the Common Rule's waiver criteria, which also require subjective determinations.

This final Rule also contains a conforming modification in § 164.512(i)(2)(iii) to replace ''(i)(2)(ii)(D)'' with ''(i)(2)(ii)(C).''

Response to Other Public Comments

Comment: It was suggested that the Department eliminate the March 2002 NPRM waiver criterion that requires IRBs or Privacy Boards to determine if there is an ''adequate plan to protect identifiers from improper use and disclosure,'' in order to avoid the IRB having to make subjective decisions.

Response: The Department disagrees with the commenter that the waiver criterion adopted in this final Rule is too subjective for an IRB or a Privacy Board to use. First, the consideration of whether there is an adequate plan to protect identifiers from improper use and disclosure is one of three factors that an IRB or Privacy Board must weigh in determining that the use or disclosure of protected health information for the research proposal involves no more than a minimal risk to the privacy of the individual. The Department does not believe that the minimal risk determination, which is based upon a similar waiver criterion in the Common Rule, is made unduly subjective by requiring the IRB to take into account the researcher's plans for maintaining the confidentiality of the information.

Second, as noted in the discussion of these provisions in the proposal, the Privacy Rule is intended to supplement and build upon the human subject protections already afforded by the Common Rule and the Food and Drug Administration's human subject protection regulations. One provision already in effect under these authorities is that, 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).) The Department, therefore, believes that IRBs and Privacy Boards are accustomed to making the type of determinations required under the Privacy Rule.

Nonetheless, as stated above, the Department is prepared to respond to actual issues that may arise during the implementation of these provisions and to provide the guidance necessary to address concerns of IRBs, Privacy Boards, and researchers in this area.

Comment: A few commenters requested elimination of the waiver element at § 164.512(i)(2)(ii)(A)(2) that would require the IRB or Privacy Board to determine that ''there is an adequate plan to destroy identifiers at the earliest opportunity consistent with the conduct of the research, unless there is a health or research justification for their retention or such retention is required by law.'' These commenters argued that this requirement may lead to premature destruction of the data, which may hinder investigations of defective data analysis or research misconduct.

Response: The waiver element at § 164.512(i)(2)(ii)(A)(2) accounts for these concerns by permitting the retention of identifiers if there is a health or research justification, or if such retention is required by law. It is expected that IRBs and Privacy Boards will consider the need for continued analysis of the data, research, and possible investigations of research misconduct when considering whether this waiver element has been met. In addition, destroying identifiers at the earliest opportunity helps to ensure that the use or disclosure of protected health information will indeed pose no more than ''minimal risk to the privacy of individuals.'' Requiring the researcher to justify the need to retain patient identifiers provides needed flexibility for research, while maintaining the goal of protecting individuals' privacy interests. If additional issues arise after implementation, the Department can most appropriately address them through guidance.

Comment: Commenters also requested clarification of the proposed waiver element at § 164.512(i)(2)(ii)(A)(3), that will require an IRB or Privacy Board to determine that there are ''adequate written assurances that the protected health information would 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.'' Specifically, the commenter's concern centered on what effect this criterion could have on retrospective studies involving data re-analysis.

Response: The Department clarifies that the Privacy Rule permits the use or disclosure of protected health information for retrospective research studies involving data re-analysis only if such use or disclosure is made either with patient authorization or a waiver of patient authorization as permitted by § 164.508 or § 164.512(i), respectively. If issues develop in the course of implementation, the Department intends to provide the guidance necessary to address these questions.

Comment: A few commenters suggested clarifying that recruitment for clinical trials by a covered entity using protected health information in the covered entity's possession is a health care operation function, not a marketing function. These commenters argued that a partial IRB or Privacy Board waiver of authorization for recruitment purposes would be too burdensome for the covered entity, and would prevent covered health care providers from communicating with their patients about the availability of clinical trials.

Response: Research recruitment is neither a marketing nor a health care operations activity. Under the Rule, a covered entity is permitted to disclose protected health information to the individual who is the subject of the information, regardless of the purpose of the disclosure. *See* § 164.502(a)(1)(i). Therefore, covered health care providers and patients may continue to discuss the option of enrolling in a clinical trial without patient authorization, and

without an IRB or Privacy Board waiver of patient authorization. However, where a covered entity wants to disclose an individual's information to a third party for purposes of recruitment in a research study, the covered entity first must obtain either authorization from that individual as required at § 164.508, or a waiver of authorization as permitted at § 164.512(i).

Comment: It was suggested that the Rule should permit covered health care providers to obtain an authorization allowing the use of protected health information for recruitment into clinical trials without specifying the person to whom the information would be disclosed and the exact information to be disclosed, but retaining the authorization requirements of specified duration and purpose, and adding a requirement for the minimum necessary use or disclosure.

Response: The Department understands that the Privacy Rule will alter some research recruitment but disagrees with the commenter's proposal to permit broad authorizations for recruitment into clinical trials. The Department decided not to adopt this suggestion because such a blanket authorization would not provide individuals with sufficient information to make an informed choice about whether to sign the authorization. In addition, adopting this change also would be inconsistent with Department's decision to eliminate the distinction in the Rule between research that includes treatment and research that does not.

Comment: It was suggested that the Department exempt from the Privacy Rule research that is already covered by the Common Rule and/or FDA's human subject protection regulations. Commenters stated that this would reduce the burden of complying with the Rule for covered entities and researchers already governed by human subject protection regulations, while requiring those not previously subject to compliance with human subject protection regulations to protect individuals' privacy.

Response: Many who commented on the December 2000 Privacy Rule argued for this option as well. The Department had previously considered, but chose not to adopt, this approach. Since the Common Rule and the FDA's human subject protection regulations contain only two requirements that specifically address confidentiality protections, the Privacy Rule will strengthen existing human subject privacy protections for research. More importantly, the Privacy Rule creates equal standards of privacy protection for research governed by the existing regulations and research that is not.

Comment: It was argued that the waiver provision should be eliminated. The commenter argued that IRBs or Privacy Boards should not have the right to waive a person's privacy rights, and that individuals should have the right to authorize all uses and disclosures of protected health information about themselves.

Response: The Department disagrees that safeguarding individuals' privacy interests requires that individuals be permitted to authorize all uses and disclosures of protected health information about themselves. In developing the Privacy Rule, the Department carefully weighed individuals' privacy interests with the need for identifiable health information for certain public policy and national priority purposes. The Department believes that the Privacy Rule reflects an appropriate balance. For example, the Rule appropriately allows for the reporting of information necessary to ensure public health, such as information about a contagious disease that may be indicative of a bioterrorism event, without individual authorization. With respect to research, the Department strongly believes that continued improvements in our nation's health require that researchers be permitted access to protected health information without individual authorization in certain limited circumstances. However, we do believe that researchers' ability to use protected health information without a patient's authorization is a privilege that requires strong confidentiality protections to ensure that the information is not misused. The Department believes that the safeguards required by the final Rule achieve the appropriate balance between protecting individuals' privacy interests, while permitting researchers to access protected health information for important, and potentially life-saving, studies.

Comment: A few commenters stated that, if the Rule permits covered entities to release protected health information to sponsor-initiated registries related to quality, safety, or effectiveness of FDA-regulated products, then this permission should apply to academic institutes and non-profit organizations as well. Otherwise, the commenters argued, the Rule establishes a double standard for research registries created by FDA-regulated entities versus registries created by academic or non-profit sponsored entities.

Response: The provisions under § 164.512(b)(iii) are intended to allow the disclosure of information to FDA-regulated entities for the limited purpose of conducting public health activities to ensure the qualify, safety, or effectiveness of FDA-regulated products, including drugs, medical devices, biological products, and food. Thus, the Department does not believe a modification to the research provisions is appropriate. The Privacy Rule permits covered entities to disclose protected health information to a registry for research purposes, including those sponsored by academic and non-profit organizations, if such disclosure: is required by law under § 164.512(a), is made pursuant to an IRB or Privacy Board waiver of authorization under § 164.512(i), is made pursuant to the individual's authorization as provided by § 164.508, or consists only of a limited data set as provided by § 164.514(e).

Comment: It was suggested that the Department modify the Rule's definition of ''research'' or the provision for preparatory research to explicitly permit the building and maintenance of research databases and repositories. The commenter further asserted that, under the Common Rule, ''research'' signifies an actual research protocol, and would not include a data or tissue compilation that is undertaken to facilitate future protocols. Therefore, since the Privacy Rule and the Common Rule have the same definition of ''research,'' this commenter was concerned that the Privacy Rule would not permit a pre-research practice in which a covered entity compiles protected health information in a systematic way to either assist researchers in their reviews that are preparatory to research, or to conduct future research.

Response: The Department does not believe such a modification is necessary. Under the Common Rule, the Office for Human Research Protections (OHRP) has interpreted the definition of ''research'' to include the development of a repository or database for future research purposes. In fact, OHRP has issued guidance on this issue, which can be found at the following URL: *http://ohrp.osophs.dhhs.gov/humansubjects/guidance/reposit.htm.* The Department interprets the definition of ''research'' in the Privacy Rule to be consistent with what is considered research under the Common Rule. Thus, the development of research repositories and databases for future research are considered research for the purposes of the Privacy Rule.

Comment: A commenter suggested eliminating the minimum necessary requirement for uses and disclosures made pursuant to a waiver of authorization by an IRB or Privacy

Board. The commenter argued that this proposal would lessen covered entities' concern that they would be held responsible for an IRB or Privacy Board's inappropriate determination and would, thus, increase the likelihood that covered entities would rely on the requesting researcher's IRB or Privacy Board documentation that patient authorization could be waived as permitted at § 164.512(i). This commenter further argued that this proposal would discourage covered entities from imposing duplicate review by the covered entities' own IRB or Privacy Board, thereby decreasing burden for covered entities, researchers, IRBs, and Privacy Boards.

Response: Although the Secretary acknowledges the concern of these commenters, the Rule at § 164.514(d)(3)(iii)(D) already permits covered entities to reasonably rely on documentation from an external IRB or Privacy Board as meeting the minimum necessary requirement, provided the documentation complies with the applicable requirements of § 164.512(i). The Department understands that covered entities may elect to require duplicate IRB or Privacy Board reviews before disclosing protected health information to requesting researchers, but has determined that eliminating the minimum necessary requirement would pose inappropriate and unnecessary risk to individuals' privacy. For example, if the covered entity has knowledge that the documentation of IRB or Privacy Board approval was fraudulent with respect to the protected health information needed for a research study, the covered entity should not be permitted to rely on the IRB or Privacy Board's documentation as fulfilling the minimum necessary requirement. Therefore, in the revised Final Rule, the Department has retained the minimum necessary requirement for research uses and disclosures made pursuant to § 164.512(i).

G. Section 164.514—Other Requirements Relating to Uses and Disclosures of Protected Health Information

1. De-Identification of Protected Health Information

December 2000 Privacy Rule. 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 requires removal of geographic subdivisions smaller than a State, except for 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. For example, the code cannot be a derivation of the individual's social security number, nor can it be 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 the need to protect individuals' identities with the need to allow de-identified databases to be useful.

March 2002 NPRM. The Department heard a number of concerns regarding the de-identification standard in the Privacy Rule. These concerns generally were raised in the context of using and disclosing information for research, public health purposes, or for certain health care operations. In particular, concerns were expressed 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 analyses for research and these other purposes. The comments, however, demonstrated little consensus as to which data elements were needed for such analyses and were largely silent regarding the feasibility of using the Privacy Rule's alternative statistical method to de-identify information.

Based on the comments received, the Department was not convinced of the need to modify the safe harbor standard for de-identified information. However, the Department was aware that a number of entities were confused by potentially conflicting provisions within the de-identification standard. These entities 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 such a re-identification code to be considered one of the unique, identifying numbers or codes that prevented the information from being de-identified. Therefore, the Department proposed a technical modification to the safe harbor provisions explicitly to except the re-identification code or other means of record identification permitted by § 164.514(c) from the listed identifiers (§ 164.514(b)(2)(i)(R)).

Overview of Public Comments. The following provides an overview of the public comment received on this proposal. Additional comments received on this issue are discussed below in the section entitled, ''Response to Other Public Comments.''

All commenters on our clarification of the safe harbor re-identification code not being an enumerated identifier supported our proposed regulatory clarification.

Final Modifications. Based on the Department's intent that the re-identification code not be considered one of the enumerated identifiers that must be excluded under the safe harbor for de-identification, and the public comment supporting this clarification, the Department adopts the provision as proposed. The re-identification code or other means of record identification permitted by § 164.514(c) is expressly excepted from the listed safe harbor identifiers at § 164.514(b)(2)(i)(R).

Response to Other Public Comments

Comment: One commenter asked if data can be linked inside the covered entity and a dummy identifier substituted for the actual identifier when the data is disclosed to the external researcher, with control of the dummy identifier remaining with the covered entity.

Response: The Privacy Rule does not restrict linkage of protected health information inside a covered entity. The model that the commenter describes for the dummy identifier is consistent with the re-identification code allowed under the Rule's safe harbor so long as the covered entity does not generate the dummy identifier using any individually identifiable information. For example, the dummy identifier cannot be derived from the individual's social security number, birth date, or hospital record number.

Comment: Several commenters who supported the creation of de-identified data for research based on removal of facial identifiers asked if a keyed-hash message authentication code (HMAC) can be used as a re-identification code even though it is derived from patient information, because it is not intended to re-identify the patient and it is not possible to identify the patient from the code. The commenters stated that use of the keyed-hash message authentication code would be valuable for research, public health and bio-terrorism detection purposes where there is a need to link clinical events on the same person occurring in different health care settings (*e.g.* to avoid double counting of cases or to observe long-term outcomes).

These commenters referenced Federal Information Processing Standard (FIPS) 198: ''The Keyed-Hash Message Authentication Code.'' This standard describes a keyed-hash message authentication code (HMAC) as a mechanism for message authentication using cryptographic hash functions. The HMAC can be used with any iterative approved cryptographic hash function, in combination with a shared secret key. A hash function is an approved mathematical function that maps a string of arbitrary length (up to a pre-determined maximum size) to a fixed length string. It may be used to produce a checksum, called a hash value or message digest, for a potentially long string or message.

According to the commenters, the HMAC can only be breached when the key and the identifier from which the HMAC is derived and the de-identified information attached to this code are known to the public. It is common practice that the key is limited in time and scope (*e.g.* only for the purpose of a single research query) and that data not be accumulated with such codes (with the code needed for joining records being discarded after the de-identified data has been joined).

Response: The HMAC does not meet the conditions for use as a re-identification code for de-identified information. It is derived from individually identified information and it appears the key is shared with or provided by the recipient of the data in order for that recipient to be able to link information about the individual from multiple entities or over time. Since the HMAC allows identification of individuals by the recipient, disclosure of the HMAC violates the Rule. It is not solely the public's access to the key that matters for these purposes; the covered entity may not share the key to the re-identification code with anyone, including the recipient of the data, regardless of whether the intent is to facilitate re-identification or not.

The HMAC methodology, however, may be used in the context of the limited data set, discussed below. The limited data set contains individually identifiable health information and is not a de-identified data set. Creation of a limited data set for research with a data use agreement, as specified in § 164.514(e), would not preclude inclusion of the keyed-hash message authentication code in the limited data set. The Department encourages inclusion of the additional safeguards mentioned by the commenters as part of the data use agreement whenever the HMAC is used.

Comment: One commenter requested that HHS update the safe harbor de-identification standard with prohibited 3-digit zip codes based on 2000 Census data.

Response: The Department stated in the preamble to the December 2000 Privacy Rule that it would monitor such data and the associated re-identification risks and adjust the safe harbor as necessary. Accordingly, the Department provides such updated information in response to the above comment. The Department notes that these three-digit zip codes are based on the five-digit zip Code Tabulation Areas created by the Census Bureau for the 2000 Census. This new methodology also is briefly described below, as it will likely be of interest to all users of data tabulated by zip code.

The Census Bureau will not be producing data files containing U.S. Postal Service zip codes either as part of the Census 2000 product series or as a post Census 2000 product. However, due to the public's interest in having statistics tabulated by zip code, the Census Bureau has created a new statistical area called the Zip Code Tabulation Area (ZCTA) for Census 2000. The ZCTAs were designed to overcome the operational difficulties of creating a well-defined zip code area by using Census blocks (and the addresses found in them) as the basis for the ZCTAs. In the past, there has been no correlation between zip codes and Census Bureau geography. Zip codes can cross State, place, county, census tract, block group and census block boundaries. The geographic entities the Census Bureau uses to tabulate data are relatively stable over time. For instance, census tracts are only defined every ten years. In contrast, zip codes can change more frequently. Because of the ill-defined nature of zip code boundaries, the Census Bureau has no file (crosswalk) showing the relationship

between US Census Bureau geography and US Postal Service zip codes.

ZCTAs are generalized area representations of U.S. Postal Service (USPS) zip code service areas. Simply put, each one is built by aggregating the Census 2000 blocks, whose addresses use a given zip code, into a ZCTA which gets that zip code assigned as its ZCTA code. They represent the majority USPS five-digit zip code found in a given area. For those areas where it is difficult to determine the prevailing five-digit zip code, the higher-level three-digit zip code is used for the ZCTA code. For further information, go to: *http://www.census.gov/geo/www/gazetteer/places2k.html.*

Utilizing 2000 Census data, the following three-digit ZCTAs have a population of 20,000 or fewer persons. To produce a de-identified data set utilizing the safe harbor method, all records with three-digit zip codes corresponding to these three-digit ZCTAs must have the zip code changed to 000. The 17 restricted zip codes are: 036, 059, 063, 102, 203, 556, 692, 790, 821, 823, 830, 831, 878, 879, 884, 890, and 893.

2. Limited Data Sets

March 2002 NPRM. As noted above, the Department heard many concerns that the de-identification standard in the Privacy Rule could curtail important research, public health, and health care operations activities. Specific concerns were raised by State hospital associations regarding their current role in using patient information from area hospitals to conduct and disseminate analyses that are useful for hospitals in making decisions about quality and efficiency improvements. Similarly, researchers raised concerns that the impracticality of using de-identified data would significantly increase the workload of IRBs because waivers of individual authorization would need to be sought more frequently for research studies even though no direct identifiers were needed for the studies. Many of these activities and studies were also being pursued for public health purposes. Some commenters urged the Department to permit covered entities to disclose protected health information for research if the protected health information is facially de-identified, that is, 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.

In response to these concerns, the Department, in the NPRM, requested comments on an alternative approach that would permit uses and disclosures of a limited data set which would not include direct identifiers but in which certain potentially identifying information would remain. The Department proposed limiting the use or disclosure of any such limited data set to research, public health, and health care operations purposes only.

From the de-identification safe harbor list of identifiers, we proposed the following as direct identifiers that would have to be removed from any limited data set: 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 proposed limited data set could 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 solicited comment on whether one or more other geographic units smaller than State, such as city, county, precinct, neighborhood or other unit, would be needed in addition to, or be preferable to, the 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 clarified that the Privacy Rule de-identification safe harbor allows disclosure of the age of an individual, including age expressed in months, days, or hours. Given that the limited data set could include all ages, including age in months, days, or hours (if preferable), the Department requested comment on whether date of birth would be needed and, if so, whether the entire date would be needed, or just the month and year.

In addition, to further protect privacy, the Department proposed 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 purposes specified in the Privacy Rule, to limit who can use or receive the data, and agree not to re-identify the data or contact the individuals.

Overview of Public Comments. The following discussion provides an overview of the public comment received on this proposal. Additional comments received on this issue are discussed below in the section entitled, ''Response to Other Public Comments.''

Almost all those who commented on this issue supported the basic premise of the limited data set for research, public health, and health care operations. Many of these commenters used the opportunity to reiterate their opposition to the safe harbor and statistical de-identification methods, and some misinterpreted the limited data set proposal as creating another safe-harbor form of de-identified data. In general, commenters agreed with the list of direct identifiers proposed in the preamble of the NPRM; some recommended changes. The requirement of a data use agreement was similarly widely supported, although a few commenters viewed it as unnecessary and others offered additional terms which they argued would make the data use agreement more effective. Others questioned the enforceability of the data use agreements.

A few commenters argued that the limited data set would present a significant risk of identification of individuals because of the increased ability to use the other demographic variables (*e.g.*, race, gender) in such data sets to link to other publicly available data. Some of these commenters also argued that the development of computer-based solutions to support the statistical method of de-identification is advancing rapidly and can support, in some cases better than the limited data set, many of the needs for research, public health and health care operations. These commenters asserted that authorization of the limited data set approach would undermine incentives to further develop statistical techniques for de-identification that may be more protective of privacy.

Most commenters who supported the limited data set concept favored including the five-digit zip code, but also wanted other geographic units smaller than a State to be included in the limited data set. Examples of other geographic units that commenters argued are needed for research, public health or health care operational purposes were county, city, full zip code, census tract, and neighborhood. Various analytical needs were cited to support these positions, such as tracking the occurrence of a particular disease to the neighborhood level or using county level data for a needs assessment of physician specialties. A few commenters opposed inclusion of the 5-digit zip code in the limited data set, recommending that the current Rule, which requires data aggregation at the 3-digit zip code level, remain the standard.

Similarly, the majority of commenters addressing the issue supported inclusion of the full birth date in the

limited data set. These commenters asserted that the full birth date was needed for longitudinal studies, and similar research, to assure accuracy of data. Others stated that while they preferred access to the full birth date, their data needs would be satisfied by inclusion of at least the month and year of birth in the limited data set. A number of commenters also opposed inclusion of the date of birth in the limited data as unduly increasing the risk of identification of individuals.

Final Modifications. In view of the support in the public comments for the concept of a limited data set, the Department determines that adoption of standards for the use and disclosure of protected health information for this purpose is warranted. Therefore, the Department adds at § 164.514(e) a new standard and implementation specifications for a limited data set for research, public health, or health care operations purposes if the covered entity (1) uses or discloses only a ''limited data set'' as defined at § 164.514(e)(2), and (2) obtains from the recipient of the limited data set a ''data use agreement'' as defined at § 164.514(e)(4). In addition, the Department adds to the permissible uses and disclosures in § 164.502(a) express reference to the limited data set standards.

The implementation specifications do not delineate the data that can be released through a limited data set. Rather, the Rule specifies the direct identifiers that must be removed for a data set to qualify as a limited data set. As with the de-identification safe harbor provisions, the direct identifiers listed apply to protected health information about the individual or about relatives, employers, or household members of the individual. The direct identifiers include all of the facial identifiers proposed in the preamble to the NPRM: (1) Name; (2) street address (renamed postal address information, other than city, State and zip code); (3) telephone and fax numbers; (4) e-mail address; (5) social security number; (6) certificate/ license numbers; (7) vehicle identifiers and serial numbers; (8) URLs and IP addresses; and (9) full face photos and any other comparable images. The public comment generally supported the removal of this facially identifying information.

In addition to these direct identifiers, the Department designates the following information as direct identifiers that must be removed before protected health information will be considered a limited data set: (1) Medical record numbers, health plan beneficiary numbers, and other account numbers; (2) device identifiers and serial numbers; and (3) biometric identifiers, including finger and voice prints. Only a few commenters specifically stated a need for some or all of these identifiers as part of the limited data set. For example, one commenter wanted an (encrypted) medical record number to be included in the limited data set to support disease management planning and program development to meet community needs and quality management. Another commenter wanted the health plan beneficiary number included in the limited data set to permit researchers to ensure that results indicating sex, gender or ethnic differences were not influenced by the participant's health plan. And a few commenters wanted device identifiers and serial numbers included in the limited data set, to facilitate product recalls and patient safety initiatives. However, the Department has not been persuaded that the need for these identifiers outweighs the potential privacy risks to the individual by their release as part of a limited data set, particularly when the Rule makes other avenues available for the release of information that may directly identify an individual.

The Department does not include in the list of direct identifiers the ''catch-all'' category from the de-identification safe harbor of ''any other unique identifying number, characteristic or code.'' While this requirement is essential to assure that the de-identification safe harbor does in fact produce a de-identified data set, it is difficult to define in advance in the context of a limited data set. Since our goal in establishing a limited data set is not to create de-identified information and since the data use agreement constrains further disclosure of the information, we determined that it would only add complexity to implementation of the limited data set with little added protection.

In response to wide public support, the Department does not designate as a direct identifier any dates related to the individual or any geographic subdivision other than street address. Therefore, as part of a limited data set, researchers and others involved in public health studies will have access to dates of admission and discharge, as well as dates of birth and death for the individual. We agree with commenters who asserted that birth date is critical for certain research, such as longitudinal studies where there is a need to track individuals across time and for certain infant-related research. Rather than adding complexity to the Rule by trying to carve out an exception for these specific situations, and other justifiable uses, we rely on the minimum necessary requirement to keep the Rule simple while avoiding abuse. Birth date should only be disclosed where the researcher and covered entity agree that it is needed for the purpose of the research. Further, even though birth date may be included with a limited data set, the Department clarifies, as it did in the preamble to the proposed rulemaking, that the Privacy Rule allows the age of an individual to be expressed in years or in months, days, or hours as appropriate.

Moreover, the limited data set may include the five-digit zip code or any other geographic subdivision, such as State, county, city, precinct and their equivalent geocodes, except for street address. We substitute for street address the term postal address information, other than city, State and zip code in order to make clear that individual elements of postal address such as street name by itself are also direct identifiers. Commenters identified a variety of needs for various geographical codes (county, city, neighborhood, census tract, precinct) to support a range of essential research, public health and health care operations activities. Some of the examples provided included the need to analyze local geographic variations in disease burdens or in the provision of health services, conducting research looking at pathogens or patterns of health risks which may need to compare areas within a single zip code, or studies to examine data by county or neighborhood when looking for external causes of disease, as would be the case for illnesses and diseases such as bladder cancer that may have environmental links. The Department agrees with these commenters that a variety of geographical designations other than five-digit zip code are needed to permit useful and significant studies and other research to go forward unimpeded. So long as an appropriate data use agreement is in place, the Department does not believe that there is any greater privacy risk in including in the limited data set such geographic codes than in releasing the five-digit zip code.

Finally, the implementation specifications adopted at § 164.514(e) require a data use agreement between the covered entity and the recipient of the limited data set. The need for a data use agreement and the core elements of such an agreement were widely supported in the public comment.

In the NPRM, we asked whether additional conditions should be added to the data use agreement. In response, a few commenters made specific

suggestions. These included prohibiting further disclosure of the limited data set except as required by law, prohibiting further disclosure without the written consent of the covered entity, requiring that the recipient safeguard the information received in the limited data set, prohibiting further disclosure unless the data has been de-identified utilizing the statistical or safe harbor methods of the Privacy Rule, and limiting use of the data to the purpose for which it was received.

In response to these comments, in the final Rule we specify that the covered entity must enter into a data use agreement with the intended recipient which establishes the permitted uses and disclosures of such information by the recipient, consistent with the purposes of research, public health, or health care operations, limits who can use or receive the data, and requires the recipient to agree not to re-identify the data or contact the individuals. In addition, the data use agreement must contain adequate assurances that the recipient use appropriate safeguards to prevent use or disclosure of the limited data set other than as permitted by the Rule and the data use agreement, or as required by law. These adequate assurances are similar to the existing requirements for business associate agreements.

Since the data use agreement already requires the recipient to limit who can use or receive the data, and to prevent uses and disclosures beyond those stated in the agreement, and since we could not anticipate all the possible scenarios under which a limited data set with a data use agreement would be created, the Department concluded that adding any of the other suggested restrictions would bring only marginal additional protection while potentially impeding some of the purposes intended for the limited data set. The Department believes the provisions of the data use agreement provide a firm foundation for protection of the information in the limited data set, but encourages and expects covered entities and data recipients to further strengthen their agreements to conform to current practices.

We do not specify the form of the data use agreement. Thus, private parties might choose to enter into a formal contract, while two government agencies might use a memorandum of understanding to specify the terms of the agreement. In the case of a covered entity that wants to create and use a limited data set for its own research purposes, the requirements of the data use agreement could be met by having affected workforce members sign an agreement with the covered entity, comparable to confidentiality agreements that employees handling sensitive information frequently sign.

A few commenters questioned the enforceability of the data use agreements. The Department clarifies that, if the recipient breaches a data use agreement, HHS cannot take enforcement action directly against that recipient unless the recipient is a covered entity. Where the recipient is a covered entity, the final modifications provide that such covered entity is in noncompliance with the Rule if it violates a data use agreement. See § 164.514(e)(4)(iii)(B). Additionally, the Department clarifies that the disclosing covered entity is not liable for breaches of the data use agreement by the recipient of the limited data set. However, similar to business associate agreements, if a covered entity knows of a pattern of activity or practice of the data recipient that constitutes a material breach or violation of the data recipient's obligation under the data use agreement, then it must take reasonable steps to cure the breach or end the violation, as applicable, and, if unsuccessful, discontinue disclosure of protected health information to the recipient and report the problem to the Secretary. And the recipient is required to report to the covered entity any improper uses or disclosures of limited data set information of which it becomes aware. We also clarify that the data use agreement requirements apply to disclosures of the limited data set to agents and subcontractors of the original limited data set recipient.

In sum, we have created the limited data set option because we believe that this mechanism provides a way to allow important research, public health and health care operations activities to continue in a manner consistent with the privacy protections of the Rule. We agree with those commenters who stated that the limited data set is not de-identified information, as retention of geographical and date identifiers measurably increases the risk of identification of the individual through matching of data with other public (or private) data sets. However, we believe that the limitations on the specific uses of the limited data set, coupled with the requirements of the data use agreement, will provide sufficient protections for privacy and confidentiality of the data. The December 2000 Privacy Rule preamble on the statistical method for de-identification discussed the data use agreement as one of the techniques identified that can be used to reduce the risk of disclosure. A number of Federal agencies that distribute data sets for research or other uses routinely employ data use agreements successfully to protect and otherwise restrict further use of the information.

We note that, while disclosures of protected health information for certain public health purposes is already allowed under § 164.512(b), the limited data set provision may permit disclosures for some public health activities not allowed under that section. These might include disease registries maintained by private organizations or universities or other types of studies undertaken by the private sector or non-profit organizations for public health purposes.

In response to comments, the Department clarifies that, when a covered entity discloses protected health information in a limited data set to a researcher who has entered into an appropriate data use agreement, the covered entity does not also need to have documentation from an IRB or a Privacy Board that individual authorization has been waived for the purposes of the research. However, the covered entity may not disclose any of the direct identifiers listed in § 164.514(e) without either the individual's authorization or documentation of an IRB or Privacy Board waiver of that authorization.

The Department further clarifies that there are other requirements in the Privacy Rule that apply to disclosure of a limited data set, just as they do to other disclosures. For example, any use, disclosure, or request for a limited data set must also adhere to the minimum necessary requirements of the Rule. The covered entity could accomplish this by, for example, requiring the data requestor, in the data use agreement, to specify not only the purposes of the limited data set, but also the particular data elements, or categories of data elements, requested. The covered entity may reasonably rely on a requested disclosure as the minimum necessary, consistent with the provisions of § 164.514(d)(3)(iii). As an example of the use of the minimum necessary standard, a covered entity who believes that another covered entity's request to include date of birth in the limited data set is not warranted is free to negotiate with the recipient about that requirement. If the entity requesting a limited data set including date of birth is not one on whose request a covered entity may reasonably rely under § 164.514(d)(3)(iii), and the covered entity believes inclusion of date of birth is not warranted, the covered entity must either negotiate a reasonably

necessary limited data set or not make a disclosure.

The Department amends § 164.514(e)(3)(ii) to make clear that a covered entity may engage a business associate to create a limited data set, in the same way it can use a business associate to create de-identified data. As with de-identified data, a business associate relationship arises even if the limited data set is not being created for the covered entity's own use. For instance, if a researcher needs county data, but the covered entity's data contains only the postal address of the individual, a business associate may be used to convert the covered entity's geographical information into that needed by the researcher. The covered entity may hire the intended recipient of the limited data set as a business associate for this purpose. That is, the covered entity may provide protected health information, including direct identifiers, to a business associate who is also the intended data recipient, to create a limited data set of the information responsive to the business associate's request.

Finally, the Department amends § 164.528 to make clear that the covered entity does not need to include disclosures of protected health information in limited data sets in any accounting of disclosures provided to the individual. Although the Department does not consider the limited data set to constitute de-identified information, all direct identifiers are removed from the limited data set and the recipient of the data agrees not to identify or contact the individual. The burden of accounting for these disclosures in these circumstances is not warranted, given that the data may not be used in any way to gain knowledge about a specific individual or to take action in relation to that individual.

Response to Other Public Comments

Comment: A small number of commenters argued that the development of computer-based solutions to support the statistical method of de-identification is advancing rapidly and can support, in some cases better than the limited data set, many of the needs for research, public health and health care operations. They also asserted that authorization of the limited data set approach will undermine incentives to further develop statistical techniques that will be more protective of privacy than the limited data set. They proposed imposing a sunset clause on the limited data set provision in order to promote use of de-identification tools.

Response: We agree that progress is being made in the development of electronic tools to de-identify protected health information. However, the information presented by commenters did not convince us that current techniques meet all the needs identified or are easy enough to use that they can have the broad application needed to support key research, public health and health care operations needs. Where de-identification can provide better outcomes than a limited data set, purveyors of such de-identification tools will have to demonstrate to covered entities the applicability and ease of use of their products. We do not believe a sunset provision on the limited data set authority is appropriate. Rather, as part of its ongoing review of the Privacy Rule in general, and the de-identification provisions in particular, the Office for Civil Rights will periodically assess the need for these provisions.

Comment: Some commenters said that if HHS clearly defines direct identifiers and facially identifiable information, there is no need for a data use agreement.

Response: We disagree. As previously noted, the resulting limited data set is not de-identified; it still contains individually identifiable health information. As a means to assure continued protection of the information once it leaves the control of the covered entity, we believe a data use agreement is essential.

Comment: Several commenters wanted to be able to have a single coordinated data use agreement between a State hospital association and its member hospitals where data collection is coordinated through the hospital association. In addition, there was concern that requiring a data use agreement and a business associate agreement in this circumstance would create an excessive and unnecessary burden.

Response: Nothing in the requirement for a data use agreement prevents a State hospital association and its member hospitals from being parties to a common data use agreement. Furthermore, that data use agreement can be combined with a business associate agreement into a single agreement that meets the requirements of both Privacy Rule provisions.

Comment: A few commenters argued that a data use agreement should not be required for data users getting a limited data set and performing data analysis as part of the Medicaid rebate validation process under which third-party data vendors, working for pharmaceutical companies, collect prescription claims data from State agencies and analyze the results for errors and discrepancies. They argued that State agencies often find entering into such contracts difficult and time consuming. Consequently, if States have to establish data use or similar agreements, then the Medicaid rebate validation process could be adversely impacted.

Response: We are not persuaded that there is a compelling reason to exempt this category of limited data set use from the requirements for a data use agreement, as compared to other important uses. The data use agreement is key to ensuring the integrity of the limited data set process and avoiding inappropriate further uses and disclosures.

Comment: One commenter stated that allowing disclosure of the limited data set without IRB or Privacy Board review would create a loophole in the Privacy Rule, with Federally funded research continuing to undergo IRB review while private research would not.

Response: The Rule continues to make no distinction between disclosure of protected health information to Federally and privately funded researchers. To obtain a limited data set from a covered entity, both Federally-funded and privately-funded researchers must enter into a data use agreement with the covered entity. One of the reasons for establishing the limited data set provisions is that the concept of ''personally identifiable information'' that triggers IRB review of research that is subject to the Common Rule does not coincide with the definition of ''individually identifiable health information'' in the Privacy Rule. The Department believes that the limited data set comes closer to the type of information not requiring IRB approval under the Common Rule than does the de-identified data set of the Privacy Rule. However, there is no uniform definition of ''personally identifiable information'' under the Common Rule; rather, as a matter of practice, it is currently set by each individual IRB.

Comment: A few commenters suggested expanding the allowable purposes for the limited data set. One commenter proposed including payment as an allowable purpose, in order to facilitate comparison of premiums charged to insured versus uninsured patients. A few commenters wanted to allow disclosures to journalists if the individual's name and social security number have been removed and if, in the context of the record or file, the identity of the patient has not been revealed. A few commenters suggested that there was no need to restrict the purpose at all as long

as there is a data use agreement. A couple of commenters wanted to extend the purpose to include creation or maintenance of research databases and repositories.

Response: If the comparison of premiums charged to different classes of patients is being performed as a health care operation of another entity, then a limited data set could be used for this purpose. It seems unlikely that this activity would occur in relation to a payment activity, so a change to include payment as a permissible purpose is not warranted. A ''payment'' activity must relate to payment for an individual and, thus, will need direct identifiers, and uses and disclosures of protected health information for such purposes is permitted under § 164.506.

With respect to disclosures to journalists, while recognizing the important role performed by newspapers and other media in reporting on public health issues and the health care system, we disagree that the purposes of the limited data set should be expanded to include journalists. A key element of the limited data set is that the recipient enter into a data use agreement that would limit access to the limited data set, prohibit any attempt to identify or contact any individual, and limit further use or disclosure of the limited data set. These limitations are inherently at odds with journalists' asserted need for access to patient information.

The suggestion to allow disclosure of a limited data set for any purpose if there is a data use agreement would undermine the purpose of the Privacy Rule to protect individually identifiable health information from unauthorized disclosures and would conflict with the requirement in the data use agreement to restrict further use to research, public health, health care operations purposes. The Department clarifies that research encompasses the establishment of research databases and repositories. Therefore, no change to the proposal is necessary.

Comment: One commenter said that HHS should not create a list of excluded direct identifiers; rather it should enunciate principles and leave it to researchers to apply the principles.

Response: The statistical method of de-identification is based on scientific principles and methods and leaves the application to the researcher and the covered entity. Unfortunately, many have viewed this approach as too complex or imprecise for broad use. To allow broad discretion in selection of variables in the creation of a limited data set would trigger the same concerns as the statistical method, because some measure of reasonableness would have to be established. Commenters have consistently asked for precision so that they would not have to worry as to whether they were in compliance with the requirements of the Privacy Rule. The commenter's proposal runs counter to this desire for precision.

Comment: One commenter wanted prescription numbers allowed in a limited data set because they do not include any ''facially identifiable information.''

Response: Prescription numbers are medical record numbers in that they are used to track an individual's encounter with a health care provider and are uniquely associated with that individual. The fact that an individual receives a new prescription number for each prescription, even if it is randomly generated, is analogous to an individual receiving a separate medical record number for different hospital visits. Thus, a prescription number is an excluded direct identifier under the medical record number exclusion for the limited data set (and also must be excluded in the creation of de-identified data).

Comment: One commenter wanted clarification that a sponsor of a multi-employer group health plan could utilize the limited data set approach for the purpose of resolving claim appeals. That commenter also suggested that if the only information that a plan sponsor received was the limited data set, the group health plan should be able to give that information to the plan sponsor without amending plan documents. In lieu of the limited data set, this commenter wanted clarification that redacted information, as delineated in their comment, is a reasonable way to meet the minimum necessary standard if the plan sponsor has certified that the plan documents have been amended pursuant to the requirements of the Privacy Rule.

Response: Uses and disclosures of a limited data set is authorized only for public health, research, and health care operations purposes. A claims appeal is more likely to be a payment function, rather than a health care operation. It is also likely to require use of protected health information that includes direct identifiers. The Department disagrees with the commenter's suggestions that the Rule should allow group health plans to disclose a limited data set to a plan sponsor without amending the plan documents to describe such disclosures. Limited data sets are not de-identified information, and thus warrant this degree of protection. Therefore, only summary health information and the enrollment status of the individual can be disclosed by the group health plan to the plan sponsor without amending the plan documents. The Privacy Rule does not specify what particular data elements constitute the minimum necessary for any particular purpose.

H. Section 164.520—Notice of Privacy Practices for Protected Health Information

December 2000 Privacy Rule. The Privacy Rule at § 164.520 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. The Rule delineates specific requirements for the content of the notice, as well as for provision of the notice. The requirements for providing notice to individuals vary based on type of covered entity and method of service delivery. For example, a covered health care provider that has a direct treatment relationship with an individual must provide the notice no later than the date of first service delivery and, if the provider maintains a physical service delivery site, must post the notice in a clear and prominent location and have it available upon request for individuals to take with them. 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. In addition, if a covered entity maintains a website, the notice must be available electronically through the web site.

March 2002 NPRM. The Department proposed 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 proposed to strengthen the notice requirements in order to preserve a valuable aspect of the consent process. The notice acknowledgment proposal was intended to create the ''initial moment'' between a covered health care provider and an individual, formerly a result of the consent requirement, when individuals may focus on information practices and privacy rights and discuss with the

provider any concerns related to the privacy of their protected health information. This ''initial moment'' also would provide an 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.

With one exception for emergency treatment situations, the proposal would require that the good faith effort to obtain the written acknowledgment be made no later than the date of first service delivery, including service delivered electronically. To address potential operational difficulties with implementing these notice requirements in emergency treatment situations, the Department proposed 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 with a direct treatment relationship with the individual from having to make a good faith effort to obtain the acknowledgment altogether in such situations.

Other than requiring that the acknowledgment be in writing, the proposal would not prescribe other details of the form of the acknowledgment or limit the manner in which a covered health care provider could obtain the acknowledgment.

The proposal also provided that, if the individual's acknowledgment of receipt of the notice could not be obtained, the covered health care provider would be required to document its good faith efforts to obtain the acknowledgment and the reason why the acknowledgment was not obtained. 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.

Overview of Public Comments. The following discussion provides an overview of the public comment received on this proposal. Additional comments received on this issue are discussed below in the section entitled, ''Response to Other Public Comments.''

In general, many commenters expressed support for the proposal to require that certain health care providers, as an alternative to obtaining prior consent, make a good faith effort to obtain a written acknowledgment from the individual of receipt of the notice. Commenters stated that even though the requirement would place some burden on certain health care providers, the proposed policy was a reasonable and workable alternative to the Rule's prior consent requirement. A number of these commenters conveyed support for the proposed flexibility of the requirement that would allow covered entities to implement the requirement in accordance with their own practices. Commenters urged that the Department not prescribe (other than that the acknowledgment be in writing) the form or content of the acknowledgment, or other requirements that would further burden the acknowledgment process. In addition, commenters viewed the proposed exception for emergency treatment situations as a practical policy.

A number of other commenters, while supportive of the Department's proposal to make the obtaining of consent optional for all covered entities, expressed concern over the administrative burden the proposed notice acknowledgment requirements would impose on certain health care providers. Some of these commenters viewed the notice acknowledgment as an unnecessary burden on providers that would not afford individuals with any additional privacy rights or protections. Thus, some commenters urged that the good faith acknowledgment not be adopted in the final Rule. As an alternative, it was suggested by some that covered entities instead be required to make a good faith effort to make the notice available to consumers.

Several commenters expressed concerns that the notice acknowledgment process would reestablish some of the same operational problems associated with the prior consent requirement. For example, commenters questioned how the requirement should be implemented when the provider's first contact with the patient is over the phone, electronically, or otherwise not face-to-face, such as with telemedecine. Accordingly, it was suggested that the good faith acknowledgment of the notice be required no later than the date of first face-to-face encounter with the patient rather than first service delivery to eliminate these perceived problems.

A few others urged that the proposed notice acknowledgment requirement be modified to allow for an individual's oral acknowledgment of the notice, so long as the provider maintained a record that the individual's acknowledgment was obtained.

Some commenters did not support the proposal's written notice acknowledgment as a suitable alternative to the consent requirement, stating that such a requirement would not provide individuals with comparable privacy protections or rights. It was stated that there are a number of fundamental differences between a consent and an acknowledgment of the notice. For example, one commenter argued that asking individuals to acknowledge receipt of the notice does not provide a comparable ''initial moment'' between the provider and the individual, especially when the individual is only asked to acknowledge receipt of the notice, and not whether they have read or understood it, or have questions. Further, commenters argued that the notice acknowledgment process would not be the same as seeking the individual's permission through a consent process. Some of these commenters urged that the Department retain the consent requirements and make appropriate modifications to fix the known operational problems associated with the requirement.

A few commenters urged that the Department strengthen the notice acknowledgment process. Some commenters suggested that the Department do so by eliminating the ''good faith'' aspect of the standard and simply requiring certain health care providers to obtain the written acknowledgment, with appropriate exceptions for emergencies and other situations where it may not be practical to do so. It was also suggested that the Department require providers to ensure that the consumer has an understanding of the information provided in the notice. One commenter suggested that this may be achieved by having individuals not only indicate whether they have received the notice, but also be asked on separate lines after each section of the notice whether they have read that section. Another commenter argued that consumers should be asked to sign something more meaningful than a notice acknowledgment, such as a ''Summary of Consumer Rights,'' which clearly and briefly summarizes the ways in which their information may be used by covered entities, as well as the key rights consumers have under the Privacy Rule.

Final Modifications. After consideration of the public comment, the Department adopts in this final Rule at § 164.520(c)(2)(ii), the proposed requirement that a covered health care provider with a direct treatment relationship with an individual make a good faith effort to obtain the individual's written acknowledgment of receipt of the notice. Other covered entities, such as health plans, are not required to obtain this acknowledgment from individuals, but may do so if they choose. The Department agrees with

those commenters who stated that the notice acknowledgment process is a workable alternative to the prior consent process, retaining the beneficial aspects of the consent without impeding timely access to quality health care. The Department continues to believe strongly that promoting individuals' understanding of privacy practices is an essential component of providing notice to individuals. Through this requirement, the Department facilitates achieving this goal by retaining the opportunity for individuals to discuss privacy practices and concerns with their health care providers. Additionally, the requirement provides individuals with an opportunity to request any additional restrictions on uses and disclosures of their health information or confidential communications, as permitted by § 164.522.

As proposed in the NPRM, the final Rule requires, with one exception, that a covered direct treatment provider make a good faith effort to obtain the written acknowledgment no later than the date of first service delivery, including service delivered electronically, that is, at the time the notice is required to be provided. During emergency treatment situations, the final Rule at § 164.520(c)(2)(i)(B) delays the requirement for provision of the notice until reasonably practicable after the emergency situation, and at § 164.520(c)(2)(ii) exempts health care providers from having to make a good faith effort to obtain an individual's acknowledgment in such emergency situations. The Department agrees with commenters that such exceptions are practical and necessary to ensure that the notice and acknowledgment requirements do not impede an individual's timely access to quality health care.

The Department also agrees with commenters that the notice acknowledgment process must be flexible and provide covered entities with discretion in order to be workable. Therefore, the final modification adopts the flexibility proposed in the NPRM for the acknowledgment requirement. The Rule requires only that the acknowledgment be in writing, and does not prescribe other details such as the form that the acknowledgment must take or the process for obtaining the acknowledgment. For example, the final Rule does not require an individual's signature to be on the notice. Instead, a covered health provider is permitted, for example, to have the individual sign a separate sheet or list, or to simply initial a cover sheet of the notice to be retained by the provider. Alternatively, a pharmacist is permitted to have the individual sign or initial an acknowledgment within the log book that patients already sign when they pick up prescriptions, so long as the individual is clearly informed on the log book of what they are acknowledging and the acknowledgment is not also used as a waiver or permission for something else (such as a waiver to consult with the pharmacist). For notice that is delivered electronically as part of first service delivery, the Department believes the provider's system should be capable of capturing the individual's acknowledgment of receipt electronically. In addition, those covered health care providers that choose to obtain consent from an individual may design one form that includes both a consent and the acknowledgment of receipt of the notice. Covered health care providers are provided discretion to design the acknowledgment process best suited to their practices.

While the Department believes that the notice acknowledgment process must remain flexible, the Department does not consider oral acknowledgment by the individual to be either a meaningful or appropriate manner by which a covered health care provider may implement these provisions. The notice acknowledgment process is intended to provide a formal opportunity for the individual to engage in a discussion with a health care provider about privacy. At the very least, the process is intended to draw the individual's attention to the importance of the notice. The Department believes these goals are better accomplished by requiring a written acknowledgment and, therefore, adopts such provision in this final modification.

Under the final modification, if an individual refuses to sign or otherwise fails to provide an acknowledgment, a covered health care provider is required to document its good faith efforts to obtain the acknowledgment and the reason why the acknowledgment was not obtained. Failure by a covered entity to obtain an individual's acknowledgment, assuming it otherwise documented its good faith effort, is not a violation of this Rule. Such reason for failure simply may be, for example, that the individual refused to sign the acknowledgment after being requested to do so. This provision also is intended to allow covered health care providers flexibility to deal with a variety of circumstances in which obtaining an acknowledgment is problematic. In response to commenters requests for examples of good faith efforts, the Department intends to provide future guidance on this and other modifications.

A covered entity is required by § 164.530(j) to document compliance with these provisions by retaining copies of any written acknowledgments of receipt of the notice or, if not obtained, documentation of its good faith efforts to obtain such written acknowledgment.

The Department was not persuaded by those commenters who urged that the Department eliminate the proposed notice acknowledgment requirements because of concerns about burden. The Department believes that the final modification is simple and flexible enough so as not to impose a significant burden on covered health care providers. Covered entities are provided much discretion to design the notice acknowledgment process that works best for their business. Further, as described above, the Department believes that the notice acknowledgment requirements are important in that they retain the important aspects of the prior consent process that otherwise would be lost in the final modifications.

In response to commenters' operational concerns about the proposed notice acknowledgment requirements, the Department clarifies that the modification as proposed and now adopted as final is intended to be flexible enough to address the various types of relationships that covered health care providers may have with the individuals to whom they provide treatment, including those treatment situations that are not face-to-face. For example, a health care provider whose first treatment encounter with a patient is over the phone satisfies the notice provision requirements of the Rule by mailing the notice to the individual no later than the day of that service delivery. To satisfy the requirement that the provider also make a good faith effort to obtain the individual's acknowledgment of the notice, the provider may include a tear-off sheet or other document with the notice that requests such acknowledgment be mailed back to the provider. The Department would not consider the health care provider in violation of the Rule if the individual chooses not to mail back an acknowledgment. The Department clarifies, however, that where a health care provider's initial contact with the patient is simply to schedule an appointment, the notice provision and acknowledgment requirements may be satisfied at the time the individual arrives at the provider's facility for his or her

appointment. For service provided electronically, the Department believes that, just as a notice may be delivered electronically, a provider should be capable of capturing the individual's acknowledgment of receipt electronically in response to that transmission.

Finally, the Department does not agree with those commenters who argued that the proposed notice acknowledgment requirements are not an adequate alternative to the prior consent requirements, nor with those who argued that the proposed acknowledgment process should be strengthened if an individual's consent is no longer required. The Department believes that the notice acknowledgment process retains the important aspects of the consent process, such as creating an opportunity for a discussion between the individual and the provider of privacy issues, including the opportunity for the individual to request restrictions on how her information may be used and disclosed as permitted by § 164.522.

Additionally, the Department believes that requiring certain health care providers to obtain the individual's acknowledgment of receipt of the notice, rather than make a good faith effort to do so, would remove the flexibility of the standard and increase the burden substantially on covered entities. Such a modification, therefore, would have the potential to cause workability and operational problems similar to those caused by the prior consent requirements. Prescribing the form or content of the acknowledgment could have the same effect. The Department believes that the notice acknowledgment process must not negatively impact timely access to quality health care.

Also, the Department agrees that it will not be easy for every individual to understand fully the information in the notice, and acknowledges that the onus of ensuring that individuals have an understanding of the notice should not be placed solely on health care providers. The Rule ensures that individuals are provided with a notice in plain language but leaves it to each individual's discretion to review the notice and to initiate a discussion with the covered entity about the use and disclosure of his or her health information or the individual's rights. However, the Department continues to believe strongly that promoting individuals' understanding of privacy practices is an essential component of providing notice to individuals. The Department anticipates that many stakeholders, including the Department, covered entities, consumer organizations, health educators, the mass media and journalists, and a host of other organizations and individuals, will be involved in educating individuals about privacy notices and practices.

Response to Other Public Comments

Comment: Several commenters requested clarification as to whether a health care provider is required to obtain from individuals a new acknowledgment of receipt of the notice if the facility changes its privacy policy.

Response: The Department clarifies that this is not required. To minimize burden on the covered direct treatment provider, the final modification intends the obtaining of the individual's acknowledgment to be consistent with the timing for provision of the notice to the individual, that is, no later than the date of first service delivery. Upon revision of the notice, the Privacy Rule requires only that the direct treatment provider make the notice available upon request on or after the effective date of the revision, and, if he maintains a physical service delivery site, to post the revised notice in a clear and prominent location in his facility. *See* § 164.520(c)(2)(iii). As the Rule does not require a health care provider to provide the revised notice directly to the individual, unless requested by the individual, a new written acknowledgment is not required at the time of revision of the notice.

Comment: A few commenters requested clarification as to how the Department intended the notice acknowledgment process to be implemented within an affiliated covered entity or an organized health care arrangement (OHCA).

Response: The requirement for an individual's written acknowledgment of the notice corresponds with the requirement that the notice be provided to the individual by certain health care providers at first service delivery, regardless of whether the notice itself is the joint notice of an OHCA, the notice of an affiliated covered entity, or the notice of one entity. With respect to an OHCA, the Privacy Rule permits covered entities that participate in an OHCA to satisfy the notice requirements through the use of a joint notice, provided that the relevant conditions of § 164.520(d) are met. Section 164.520(d)(3) further provides that provision of a joint notice to an individual by any one of the covered entities included in the joint notice satisfies the notice provision requirements at § 164.520(c) with respect to all others covered by the joint notice. Thus, a health care provider with a direct treatment relationship with an individual that is participating in an OHCA only need make a good faith effort to obtain the individual's acknowledgment of the joint notice if that provider is the covered entity within the OHCA that is providing the joint notice to the individual. Where the joint notice is provided to the individual by a participating covered entity other than a provider with a direct treatment relationship with the individual, no acknowledgment need be obtained. However, covered entities that participate in an OHCA are not required to utilize a joint notice and may maintain separate notices. In such case, each covered health care provider with a direct treatment relationship within the OHCA must make a good faith effort to obtain the individual's acknowledgment of the notice he or she provides.

Similarly, an affiliated covered entity may have one single notice that covers all of its affiliates. Thus, if the affiliated covered entity's notice is provided to the individual by a health care provider with which the individual has a direct treatment relationship, the health care provider must make a good faith effort to obtain the individual's acknowledgment of receipt of the notice. Alternatively, where the affiliated entity's notice is provided to the individual by a participating entity other than a provider with a direct treatment relationship with the individual, no acknowledgment need be obtained. However, as with the OHCA, the Department clarifies that covered entities that are part of an affiliated covered entity may maintain separate notices if they choose to do so; if they do so, each provider with a direct treatment relationship with the individual must make a good faith effort to obtain the individual's acknowledgment of the notice he or she provides.

Comment: It was suggested that if a provider chooses to obtain consent, the provider should not also be required to obtain the individual's acknowledgment of the notice.

Response: For those covered entities that choose to obtain consent, the Rule does not prescribe any details of the form or manner in which the consent must be obtained. Given this discretion, the Department does not believe that all consents will provide the same benefits to the individual as those afforded by the notice acknowledgment process. The Rule, therefore, does not relieve a covered health care provider of his obligations with respect to obtaining an individual's acknowledgment of the

notice if that provider also obtains the individual's consent. However, the Rule provides those covered health care providers that choose to obtain consent from an individual the discretion to design one form that includes both a consent and the acknowledgment of receipt of the notice.

Comment: Some commenters asked that the Privacy Rule allow the written acknowledgment of the notice to be obtained electronically without regard to channel of delivery (electronically or on paper) of the notice.

Response: Generally, the Privacy Rule allows for electronic documents to qualify as written documents for purposes of meeting the Rule's requirements. This also applies with respect to the notice acknowledgment. For notice delivered electronically, the Department intends a return receipt or other transmission from the individual to suffice as the notice acknowledgment.

For notice delivered on paper in a face-to-face encounter with the provider, although it is unclear to the Department how exactly the provider may do so, the Rule does not preclude providers from obtaining the individual's written acknowledgment electronically. The Department cautions, however, that the notice acknowledgment process is intended to alert individuals to the importance of the notice and provide them the opportunity to discuss privacy issues with their providers. To ensure that individuals are aware of the importance of the notice, the Rule requires that the individual's acknowledgment be in writing. Thus, the Department would not consider a receptionist's notation in a computer system to be an individual's written acknowledgment.

Comment: One commenter expressed concern that the Rule did not define ''emergency'' as it applies to ambulance services given the Rule's exceptions to the notice requirements for such situations. This commenter also urged that the Rule's notice provisions at § 164.520(c)(2) with respect to emergency treatment situations be expanded also to apply to non-emergency trips of ambulance providers. The commenter explained that even in non-emergency circumstances, patients, especially the elderly, often suffer from incapacitating or stressful conditions when they need to be transferred by ambulance, at which time it may not be effective or appropriate to provide the notice and obtain the individual's acknowledgment of receipt of the notice.

Response: During emergency treatment situations, the final Rule at § 164.520(c)(2)(i)(B) delays the requirement for provision of the notice until reasonably practicable after the emergency situation, and exempts health care providers from having to make a good faith effort to obtain an individual's acknowledgment. As the provisions are not intended to apply only to ambulance providers, the Department does not believe that defining emergency with respect to such providers is appropriate or necessary. Nor does the Department believe that expanding these provisions to cover non-emergency trips of ambulance providers is appropriate. The provisions are intended to provide exceptions for those situations where providing the notice and obtaining an individual's acknowledgment may not be feasible or practicable. Where such extenuating circumstances do not exist, the Department expects that covered health care providers are able to provide individuals with a notice and make a good faith effort to obtain their acknowledgment of receipt. Where an individual does not provide an acknowledgment, the Rule requires only that the provider document his good faith effort to obtain the acknowledgment.

Comment: A number of commenters requested clarification on how to implement the ''good faith'' standard and urged the Department to provide more specific guidance and examples. Some commenters expressed concern over the perceived liability that would arise from such a discretionary standard.

Response: Covered entities are provided much discretion to implement the notice acknowledgment process as best suited to their specific business practices. The standard is designed as a ''good faith effort'' standard because the Department understands that obtaining an individual's acknowledgment of the notice may not always be feasible or practical, in spite of a covered entity's efforts. Thus, the standard is intended to account for those difficult situations, including where an individual simply refuses to provide the written acknowledgment. Given the discretion covered health care providers have in implementing these standards and the various ways such providers interact with their patients, it is difficult for the Department to provide specific guidance in this area that is generally applicable to many covered health care providers. However, the Department intends to provide future guidance through frequently asked questions or other materials in response to specific scenarios that are raised by industry.

With respect to commenters' concerns regarding potential liability, the Department's position is that a failure by a covered entity to obtain an individual's acknowledgment, assuming it otherwise documented its good faith effort (as required by § 164.520(c)(2)(ii)), will not be considered a violation of this Rule.

Comment: Many commenters generally urged that the Department modify the Rule to allow for a simpler, shorter, and, therefore, more readable notice. Some of the commenters explained that a shorter notice would assure that more individuals would take the time to read and be able to understand the information. Others suggested that a shorter notice would help to alleviate burden on the covered entity. A number of these commenters suggested that the Department allow for a shorter summary or 1-page notice to replace the prescriptive notice required by the Privacy Rule. It was recommended that such a notice could refer individuals to a more detailed notice, available on request, or to an HHS web site, for additional information about an individual's rights under the Privacy Rule. Others recommended that the Department allow for a layered notice that contains: (1) A short notice that briefly describes, for example, the entity's principal uses and disclosures of an individual's health information, as well as the individual's rights with respect to that information; and (2) a longer notice, layered beneath the short notice, that contains all the elements required by the Rule.

Certain other commenters urged that one way to make the notice shorter, as well as to alleviate burden on the covered entity, would be to eliminate the requirement that the notice explain the more stringent State privacy laws. Commenters stated that companies that operate in multiple States will have to develop and print up to 50 different notices, and then update and reissue those notices whenever a material change is made to the State law. These commenters recommended instead that the notice simply state that State law may provide additional protections.

A few commenters urged that the Department provide a model notice that covered entities could use in their implementation efforts.

Response: The Department does not modify the notice content provisions at § 164.520(b). The Department believes that the elements required by § 164.520(b) are important to fully inform the individual of the covered entity's privacy practices, as well as his or her rights. However, the Department agrees that such information must be provided in a clear, concise, and easy to

understand manner. Therefore, the Department clarifies that covered entities may utilize a ''layered notice'' to implement the Rule's provisions, so long as the elements required by § 164.520(b) are included in the document that is provided to the individual. For example, a covered entity may satisfy the notice provisions by providing the individual with both a short notice that briefly summarizes the individual's rights, as well as other information; and a longer notice, layered beneath the short notice, that contains all the elements required by the Privacy Rule. Covered entities, however, while encouraged to use a layered notice, are not required to do so. Nothing in the final modifications relieve a covered entity of its duty to provide the entire notice in plain language so the average reader can understand it. *See* § 164.520(b)(1).

In response to comments regarding a model notice, it would be difficult for the Department to develop a document that would be generally useful to many different types of covered entities. A covered entity's notice must reflect in sufficient detail the particular uses and disclosures that entity may make. Such uses and disclosures likely will be very different for each type of covered entity. Thus, a uniform, model notice could not capture the wide variation in information practices across covered entities. The Department intends, however, to issue further general guidance to help covered entities implement the notice provisions of the Rule.

Comment: A number of commenters also requested that the Department lessen the burden associated with distributing the notice. For example, some commenters asked that covered entities be permitted to satisfy the notice provision requirements by posting the notice at the facility or on a web site and by providing a copy only to those consumers who request one, or by placing copies on display where an interested consumer may take one.

Response: The Department's position that making the notice available to individuals, either on request, by posting it at a facility or on a web site, or by placing copies on display, does not substitute for physically providing the notice directly to individuals. Adequate notice of privacy practices is a fundamental right afforded individuals by the Rule. As such, the Department does not believe that the burden of obtaining such information should be placed on the individual. Covered entities are required to distribute the notice in the manner described under § 164.520(c).

Comment: A few commenters requested that the Department make clear that no special mailings are required to provide individuals with a covered entity's notice; rather, that the notice may be distributed as part of other mailings or distributions by the covered entity. For example, one commenter argued that the Rule should be flexible enough to allow for notices to be included in a health plan's Summary Plan Descriptions, Booklets, or an Enrollment Application. It was argued that the notice would receive greater attention, be more carefully reviewed and, thus, better understood if it were published in materials known to be widely read by members.

Response: The Department clarifies that no special or separate mailings are required to satisfy the notice distribution requirements. The Privacy Rule provides covered entities with discretion in this area. A health plan distributing its notice through the mail, in accordance with § 164.520(c)(1), may do so as part of another mailing to the individual. In addition, a covered entity that provides its notice to an individual by e-mail, in accordance with § 164.520(c)(3), may include additional materials in the e-mail. No separate e-mail is required. However, the Privacy Rule at § 164.508(b)(3) continues to prohibit a covered entity from combining the notice in a single document with an authorization.

Comment: Commenters also urged that the Rule permit, for group products, a health plan to send its notice to the administrator of the group product or the plan sponsor, who would then be responsible for distributing the notice to each enrollee/employee. One commenter claimed this distribution method is especially appropriate where there is no regular communication with the covered individuals, as in an employer-pay-all group medical or dental plan. According to the commenter, providing the notice to the employer makes sense because the employer picks the plan and should be aware of the plan's privacy practices when doing so.

Response: The Privacy Rule requires a health plan to distribute its notice to each individual covered by the plan. Health plans may arrange to have another entity, or person, for example, a group administrator or a plan sponsor, distribute the notice on their behalf. However, the Department cautions that if such other entity or person fails to distribute the notice to individuals, the health plan would be in violation of the Rule.

Comment: Another commenter asked that the Department eliminate the requirement that a covered entity must provide the notice to every dependent, rather than just the head of the household. This commenter argued that while it makes sense to provide the notice to an emancipated minor or to a minor who pursuant to State law has consented to treatment, it does not make sense to send the notice to a 2-year old child.

Response: The Privacy Rule provides that a health plan may satisfy the notice provision requirements by distributing the notice to the named insured of a policy under which coverage is provided to the named insured and one or more dependents. A health plan is not required to distribute the notice to each dependent. *See* § 164.520(c)(1)(iii).

Further, a covered health care provider with a direct treatment relationship with the individual is required only to provide the notice to the individual receiving treatment at first service delivery. Where a parent brings a 2-year old child in for treatment, the provider satisfies the notice distribution requirements by providing the notice only to the child's parent.

I. Section 164.528—Accounting of Disclosures of Protected Health Information

December 2000 Privacy Rule. 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 individual must request an accounting of disclosures.

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; and (2) for each disclosure: the date of the disclosure; the name of the entity or person who received the protected health information, and, 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 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.

March 2002 NPRM. In response to concerns about the high costs and administrative burdens associated with the requirement to account to individuals for the covered entity's disclosure of protected health information, the Department proposed 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 proposed to alleviate burden in this way because, like disclosures of protected health information made directly to the individual—which are already excluded from the accounting provisions in § 164.528(a)(1)—disclosures made pursuant to an authorization are also known by the individual, in as much as the individual was required to sign the forms authorizing the disclosures.

In addition to the exception language at § 164.528(a)(1), the Department proposed 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.

Overview of Public Comments. The following discussion provides an overview of the public comment received on this proposal. Additional comments received on this issue are discussed below in the section entitled, ''Response to Other Public Comments.''

The majority of comments on the accounting proposal supported the elimination of the accounting for authorized disclosures. The commenters agreed that, on balance, since the individual had elected to authorize the disclosure in the first instance, and that election was fully informed and voluntary, subsequently accounting for the disclosure made pursuant to that authorization was not necessary.

Many of the commenters went on to suggest other ways in which the accounting requirement could be made less burdensome. For example, several commenters wanted some or all of the disclosures which are permitted at § 164.512 without individual consent or authorization to also be exempt from the accounting requirements. Others proposed alternative means of accounting for disclosures for research, particularly when such disclosures involve large numbers of records. These commenters argued that accounting for each individual record disclosed for a large research project would be burdensome and may deter covered entities from participating in such research. Rather than an individual accounting, the commenters suggested that the covered entity be required only to disclose a listing of all relevant protocols under which an individual's information may have been released during the accounting period, the timeframes during which disclosures were made under a protocol, and the name of the institution and researcher or investigator responsible for the protocol, together with contact information for the researcher. The National Committee on Vital Health Statistics, while not endorsing a protocol listing directly, recommended the Department consider alternatives to minimize the burden of the accounting requirements on research.

Finally, several commenters objected to the elimination of the accounting requirement for authorized disclosures. Some of these commenters expressed concern that the proposal would eliminate the requirement to account for the authorized disclosure of psychotherapy notes. Others were primarily concerned that the proposal would weaken the accounting rights of individuals. According to these commenters, informing the individual of disclosures was only part of the purpose of an accounting. Even with regard to authorized disclosures, an accounting could be important to verify that disclosures were in accord with the scope and purpose as stated in the authorization and to detect potentially fraudulent, altered, or otherwise improperly accepted authorizations. Since authorizations had to be maintained in any event, accounting for these disclosures represented minimal work for the covered entity.

Final Modifications. Based on the general support in the public comment, the Department adopts the modification to eliminate the accounting requirement for authorized disclosures. The authorization process itself adequately protects individual privacy by assuring that the individual's permission is given both knowingly and voluntarily. The Department agrees with the majority of commenters that felt accounting for authorized disclosures did not serve to add to the individual's knowledge about disclosures of protected health information. The Department does recognize the role of accounting requirements in the detection of altered or fraudulent authorizations. However, the Department considers the incidence of these types of abuses, and the likelihood of their detection through a request for an accounting, to be too remote to warrant the burden on all covered entities of including authorized disclosures in an accounting. As noted by some commenters, the covered entity must retain a copy of the authorization to document their disclosure of protected health information and that documentation would be available to help resolve an individual's complaint to either the covered entity or the Secretary.

Specific concern about the elimination of the accounting requirement for authorized disclosures was expressed by mental health professionals, who believed their patients should always have the right to monitor access to their personal information. The Department appreciates theses commenters' concern about the need for heightened protections and accountability with regard to psychotherapy notes. It is because of these concerns that the Rule requires, with limited exceptions, individual authorization for even routine uses and disclosures of psychotherapy notes by anyone other than the originator of the notes. The Department clarifies that nothing in modifications adopted in this rulemaking prevents a mental health professional from including authorized disclosures of psychotherapy notes in an accounting requested by their patients. Indeed, any covered entity may account to the individual for disclosures based on the individual's authorization. The modification adopted by the Department simply no longer requires such an accounting.

In response to comment on this proposal, as well as on the proposals to permit incidental disclosures and disclosures of protected health information, other than direct identifiers, as part of a limited data set, the Department has added two additional exclusions to the accounting requirements. Disclosures that are part of a limited data set and disclosures that are merely incidental to another permissible use or disclosure will not require an accounting. The limited data set does not contain any protected health information that directly identifies the individual and the individual is further protected from identification by the required data use

agreement. The Department believes that accounting for these disclosures would be too burdensome. Similarly, the Department believes that it is impracticable to account for incidental disclosures, which by their very nature, may be uncertain or unknown to the covered entity at the time they occur. Incidental disclosures are permitted as long as reasonable safeguards and minimum necessary standards have been observed for the underlying communication. Moreover, incidental disclosures may most often happen in the context of a communication that relates to treatment or health care operations. In that case, the underlying disclosure is not subject to an accounting and it would be arbitrary to require an accounting for a disclosure that was merely incidental to such a communication.

The Department however disagrees with commenters who requested that other public purpose disclosures not be subject to the accounting requirement. Although the Rule permits disclosure for a variety of public purposes, they are not routine disclosures of the individual's information. The accounting requirement was designed as a means for the individual to find out the non-routine purposes for which his or her protected health information was disclosed by the covered entity, so as to increase the individual's awareness of persons or entities other than the individual's health care provider or health plan in possession of this information. To eliminate some or all of these public purposes would defeat the core purpose of the accounting requirement.

The Department disagrees with commenters' proposal to exempt all research disclosures made pursuant to a waiver of authorization from the accounting requirement. Individuals have a right to know what information about them has been disclosed without their authorization, and for what purpose(s). However, the Department agrees that the Rule's accounting requirements could have the undesired effect of causing covered entities to halt disclosures of protected health information for research. Therefore, the Department adopts commenters' proposal to revise the accounting requirement at § 164.528 to permit covered entities to meet the requirement for research disclosures if they provide individuals with a list of all protocols for which the patient's protected health information may have been disclosed for research pursuant to a waiver of authorization under § 164.512(i), as well as the researcher's name and contact information. The Department agrees with commenters that this option struck the appropriate balance between affirming individuals' right to know how information about them is disclosed, and ensuring that important research is not halted.

The Department considered and rejected a similar proposal by commenters when it adopted the Privacy Rule in December 2000. While recognizing the potential burden for research, the Department determined that the individual was entitled to the same level of specificity in an accounting for research disclosures as any other disclosure. At that time, however, the Department added the summary accounting procedures at § 164.528(b)(3) to address the burden issues of researchers and others in accounting for multiple disclosures to the same entity. In response to the Department's most recent request for comments, researchers and others explained that the summary accounting procedures do not address the burden of having to account for disclosures for research permitted by § 164.512(i). These research projects usually involve many records. It is the volume of records for each disclosure, not the repeated nature of the disclosures, that presents an administrative obstacle for research if each record must be individually tracked for the accounting. Similarly, the summary accounting procedures do not relieve the burden for covered entities that participate in many different studies on a routine basis. The Department, therefore, reconsidered the proposal to account for large research projects by providing a list of protocols in light of these comments.

Specifically, the Department adds a paragraph (4) to § 164.528(b) to provide for simplified accounting for research disclosures as follows:

(1) The research disclosure must be pursuant to § 164.512(i) and involve at least 50 records. Thus, the simplified accounting procedures may be used for research disclosures based on an IRB or Privacy Board waiver of individual authorization, the provision of access to the researcher to protected health information for purposes preparatory to research, or for research using only records of deceased individuals. The large number of records likely to be disclosed for these research purposes justifies the need for the simplified accounting procedures. The Department has determined that a research request for 50 or more records warrants use of these special procedures.

(2) For research protocols for which the individual's protected health information may have been disclosed during the accounting period, the accounting must include the name of the study or protocol, a description of the purpose of the study and the type of protected health information sought, and the timeframe of disclosures in response to the request.

(3) When requested by the individual, the covered entity must provide assistance in contacting those researchers to whom it is likely that the individual's protected health information was actually disclosed.

Support for streamlining accounting for research disclosures came in comments and from NCVHS. The Department wants to encourage research and believes protections afforded information in hands of researcher, particularly research overseen by IRB or Privacy Board, provides assurance of continued confidentiality of information. The Department does not agree that the individual has no need to know that his or her information has been disclosed for a research purpose. Covered entities, of course, may account for research disclosures in the same manner as all other disclosures. Even when the covered entity elects to use the alternative of a protocol listing, the Department encourages covered entities to provide individuals with disclosure of the specific research study or protocol for which their protected health information was disclosed, and other specific information relating to such actual disclosures if they so choose. If the covered entity lists all protocols for which the individual's information may have been disclosed, the Department would further encourage that the covered entity list under separate headings, or on separate lists, all protocols relating to particular health issues or conditions, so that individuals may more readily identify the specific studies for which their protected health information is more likely to have been disclosed.

The Department intends to monitor the simplified accounting procedures for certain research disclosures to determine if they are effective in providing meaningful information to individuals about how their protected health information is disclosed for research purposes, while still reducing the administrative burden on covered entities participating in such research efforts. The Department may make adjustments to the accounting procedures for research in the future as necessary to ensure both goals are fully met.

Response to Other Public Comments

Comment: A few commenters opposed the proposal to eliminate the accounting requirement for all

authorized disclosures arguing that, absent a full accounting, the individual cannot meaningfully exercise the right to amend or to revoke the authorization. Others also felt that a comprehensive right to an accounting, with no exceptions, was better from an oversight and enforcement standpoint as it encouraged consistent documentation of disclosures. One commenter also pointed to an example of the potential for fraudulent authorizations by citing press accounts of a chain drug store that allegedly took customers signatures from a log that waived their right to consult with the pharmacist and attached those signatures to a form authorizing the receipt of marketing materials. Under the proposal, the commenter asserted, the chain drug store would not have to include such fraudulent authorizations as part of an accounting to the individual.

Response: The Department does not agree that the individual's right to amendment is materially affected by the accounting requirements for authorized disclosures. The covered entity that created the protected health information contained in a designated record set has the primary obligation to the individual to amend any erroneous or incomplete information. The individual does not necessarily have a right to amend information that is maintained by other entities that the individual has authorized to have his or her protected health information. Furthermore, the covered entity that has amended its own designated record set at the request of the individual is obligated to make reasonable efforts to notify other persons, including business associates, that are known to have the protected health information that was the subject of the amendment and that may rely on such information to the detriment of the individual. This obligation would arise with regard to persons to whom protected health information was disclosed with the individual's authorization. Therefore, the individual's amendment rights are not adversely affected by the modifications to the accounting requirements. Furthermore, nothing in the modification adversely affects the individual's right to revoke the authorization.

The Department agrees that oversight is facilitated by consistent documentation of disclosures. However, the Department must balance its oversight functions with the burden on entities to track all disclosures regardless of purpose. Based on this balancing, the Department has exempted routine disclosures, such as those for treatment, payment, and health care operations, and others for security reasons. The addition of authorized disclosures to the exemption from the accounting does not materially affect the Department's oversight function. Compliance with the Rule's authorization requirements can still be effectively monitored because covered entities are required to maintain signed authorizations as documentation of disclosures. Therefore, the Department believes that effective oversight, not the happenstance of discovery by an individual through the accounting requirement, is the best means to detect and prevent serious misdeeds such as those alleged in fraudulent authorizations.

Comment: A number of commenters recommended other types of disclosures for exemption from the accounting requirement. Many recommended elimination of the accounting requirement for public health disclosures arguing that the burden of the requirement may deter entities from making such disclosures and that because many are made directly to public health authorities by doctors and nurses, rather than from a central records component of the entity, public health disclosures are particularly difficult to track and document. Others suggested exempting from an accounting requirement any disclosure required by another law on the grounds that neither the individual nor the entity has any choice about such required disclosures. Still others wanted all disclosures to a governmental entity exempted as many such disclosures are required and often reports are routine or require lots of data. Some wanted disclosures to law enforcement or to insurers for claims investigations exempted from the accounting requirement to prevent interference with such investigatory efforts. Finally, a few commenters suggested that all of the disclosures permitted or required by the Privacy Rule should be excluded from the accounting requirement.

Response: Elimination of an accounting requirement for authorized disclosures is justified in large part by the individual's knowledge of and voluntary agreement to such disclosures. None of the above suggestions for exemption of other permitted disclosures can be similarly justified. The right to an accounting of disclosures serves an important function in informing the individual as to which information was sent to which recipients. While it is possible that informing individuals about the disclosures of their health information may on occasion discourage some worthwhile activity, the Department believes that the individual's right to know who is using their information and for what purposes takes precedence.

Comment: One commenter sought an exemption from the accounting requirement for disclosures to adult protective services when referrals are made for abuse, neglect, or domestic violence victims. For the same reasons that the Rule permits waiver of notification to the victim at the time of the referral based on considerations of the victim's safety, the regulation should not make such disclosures known after the fact through the accounting requirement.

Response: The Department appreciates the concerns expressed by the commenter for the safety and welfare of the victims of abuse, neglect, or domestic violence. In recognition of these concerns, the Department does give the covered entity discretion in notifying the victim and/or the individual's personal representative at the time of the disclosure. These concerns become more attenuated in the context of an accounting for disclosures, which must be requested by the individual and for which the covered entity has a longer timeframe to respond. Concern for the safety of victims of abuse or domestic violence should not result in stripping these individuals of the rights granted to others. If the individual is requesting the accounting, even after being warned of the potential dangers, the covered entity should honor that request. However, if the request is by the individual's personal representative and the covered entity has a reasonable belief that such person is the abuser or that providing the accounting to such person could endanger the individual, the covered entity continues to have the discretion in § 164.502(g)(5) to decline such a request.

Comment: One commenter suggested elimination of the accounting requirement in its entirety. The commenter argued that HIPAA does not require an accounting as the individual's right and the accounting does not provide any additional privacy protections to the individual's information.

Response: The Department disagrees with the commenter. HIPAA authorized the Secretary to identify rights of the individual with respect to protected health information and how those rights should be exercised. In absence of regulation, HIPAA also authorized the Secretary to effectuate these rights by regulation. As stated in the preamble to the December 2000 Privacy Rule, the standard adopted by the Secretary that provides individuals with a right to an

accounting of disclosures, is consistent with well-established privacy principles in other law and with industry standards and ethical guidelines, such as the Federal Privacy Act (5 U.S.C. 552a), the July 1977 Report of the Privacy Protection Study Commission, and NAIC Health Information Privacy Model Act. (*See* 65 FR 82739.)

Comment: A few commenters requested that the accounting period be shortened from six years to two years or three years.

Response: The Department selected six years as the time period for an accounting to be consistent with documentation retention requirements in the Rule. We note that the Rule exempts from the accounting disclosures made prior to the compliance date for Rule, or April 14, 2003. Therefore, it will not be until April 2009 that a full six year accounting period will occur. Also, the Rule permits individuals to request and the covered entity to provide for an accounting for less than full six year period. For example, an individual may be interested only in disclosures that occurred in the prior year or in a particular month. The Department will monitor the use of the accounting requirements after the compliance date and will evaluate the need for changes in the future if the six year period for the accounting proves to be unduly burdensome.

Comment: Commenters requested clarification of the need to account for disclosures to business associates, noting that while the regulation states that disclosures to and by a business associate are subject to an accounting, most such disclosures are for health care operations for which no accounting is required.

Response: The Department clarifies that the implementation specification in § 164.528(b)(1), that expressly includes in the content of an accounting disclosures to or by a business associate, must be read in conjunction with the basic standard for an accounting for disclosures in § 164.528(a). Indeed, the implementation specification expressly references the standard. Read together, the Rule does not require an accounting of any disclosure to or by a business associate that is for any exempt purpose, including disclosures for treatment, payment, and health care operations.

Comment: One commenter wanted health care providers to be able to charge reasonable fees to cover the retrieval and preparation costs of an accounting for disclosures.

Response: In granting individuals the right to an accounting, the Department had to balance the individual's right to know how and to whom protected health information is being disclosed and the financial and administrative burden on covered entities in responding to such requests. The balance struck by the Department with regard to cost was to grant the individual a right to an accounting once a year without charge. The covered entity may impose reasonable, cost-based fees for any subsequent requests during the one year period. The Department clarifies that the covered entity may recoup its reasonable retrieval and report preparation costs, as well as any mailing costs, incurred in responding to subsequent requests. The Rule requires that individuals be notified in advance of these fees and provided an opportunity to withdraw or amend its request for a subsequent accounting to avoid incurring excessive fees.

Comment: One commenter wanted clarification of the covered entity's responsibility to account for the disclosures of others. For example, the commenter wanted to know if the covered entity was responsible only for its own disclosures or did it also need to account for disclosures by every person that may subsequently handle the information.

Response: The Department clarifies in response to this comment that a covered entity is responsible to account to the individual for certain disclosures that it makes and for disclosures by its business associates. The covered entity is not responsible to account to the individual for any subsequent disclosures of the information by others that receive the information from the covered entity or its business associate.

J. Section 164.532—Transition Provisions

1. Research Transition

December 2000 Privacy Rule. The December 2000 Privacy Rule at § 164.532 contained different transition requirements for research being conducted with an individual's legal permission that included treatment, and for research being conducted with an individual's legal permission that did not include treatment. However, the Rule did not explicitly address transition provisions for research studies ongoing after the compliance date where the legal permission of the individual had not been sought.

March 2002 NPRM. Several commenters found the transition provisions for research to be confusing, and further noted that December 2000 Privacy Rule did not address research ongoing after the compliance date where the legal permission of the individual had not been sought. To address these concerns, the Department proposed several revisions to the Privacy Rule's transition provisions. In particular, the Department proposed that there be no distinction in the transition provisions between research that includes treatment and research that does not, and no distinction between the requirements for research conducted with a patient's legal permission and research conducted with an IRB-approved waiver of a patient's informed consent. In sum, the NPRM proposed that covered entities be permitted to use or disclose protected health information created or received for a specific research study before the compliance date (if there was no agreed-to restriction in accordance with § 164.522(a)), if the covered entity has obtained, prior to the compliance date, any one of the following: (1) An 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 the Common Rule or FDA's human subject protection regulations. However, even if the researcher obtained, from an IRB, a waiver of informed consent, an authorization would be required if informed consent is later obtained. This may occur if there is a temporary waiver of informed consent for emergency research under the Food and Drug Administration human subject protection regulations.

Overview of Public Comments. The following discussion provides an overview of the public comment received on this proposal. Additional comments received on this issue are discussed below in the section entitled, ''Response to Other Public Comments.''

Most commenters supported the proposed revisions to the Privacy Rule's transition provisions for research. However, a few commenters requested that the transition provisions be broadened to permit covered entities to rely on an express legal permission or informed consent approved by an IRB before the compliance date, even if the permission or consent had not been signed by the individual prior to the compliance date. Consequently, a researcher could use the same forms throughout their study, decreasing the chance of introducing error into the research through the use of multiple recruitment procedures, disruption to the research, and the burden for the IRBs and researchers. A few other

commenters suggested that covered entities be permitted to use and disclose protected health information with consent forms approved by an IRB prior to the compliance date until the next review by the IRB, as required by the Common Rule. They argued that this would result in all informed consent forms being in compliance with the Privacy Rule's authorization regulations within a one-year period, and it would avoid disruption to ongoing research, as well as a flood of consent form revision requests to the IRBs.

Final Modifications. The Department agrees with the majority of comments that supported the modifications to the transition provisions, and has therefore adopted the research transition modifications as proposed in the NPRM. The Department disagrees with the comments that suggest broadening the transition provisions to permit covered entities to rely on an express legal permission or informed consent that had not been signed by the individual before the compliance date. The Department understands that this provision may disrupt some ongoing research; however, the recruitment periods for some studies may continue long after the compliance date, and it would be unreasonable to grandfather-in existing informed consent documents indefinitely. While the commenter's suggestion to only grandfather-in such informed consent documents until the next review by the IRB would address this concern, the Privacy Rule does not require initial or continuing IRB or Privacy Board review of authorization forms or informed consent documents. Therefore, the Department does not adopt this change to its proposal.

However, the Department understands that some existing express legal permissions, informed consents, or IRB-approved waivers of informed consents are not study specific. Therefore, the final Rule permits covered entities to rely on an express legal permission, informed consent, or IRB-approved waiver of informed consent for future unspecified research, provided the legal permission, informed consent or IRB-approved waiver was obtained prior to the compliance date.

Response to Other Public Comments

Comment: A commenter requested that the transition provision be narrowed by requiring research that received a waiver of informed consent from an IRB prior to the compliance date but that begins after the compliance date be re-evaluated under the Privacy Rule's waiver criteria.

Response: The Department disagrees. Given that the Privacy Rule's waiver criteria for an individual's authorization generally are consistent with the same types of considerations currently applied to a waiver of an individual's informed consent, this suggestion would impose unnecessary burdens on researchers, IRBs, and Privacy Boards, with respect to the few research studies that would fall in this category.

2. Business Associates

December 2000 Privacy Rule. 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 use the services of, or receive assistance from, 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 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 is in noncompliance with the Privacy Rule.

The Privacy Rule's definition of ''business associate'' at § 160.103 includes the types of functions or activities, and list 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).

March 2002 NPRM. The Department heard concerns from many covered entities and others about the business associate provisions of the Privacy Rule. The majority expressed some concern over the anticipated administrative burden and cost to implement the business associate provisions. Some stated that many covered entities have existing contracts that are not set to terminate or expire until after the compliance date of the Privacy Rule. Others 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. These entities went on to urge 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 concerns, the Department proposed to relieve some of the burden on covered entities in complying with the business associate provisions by both adding a transition provision to grandfather certain existing contracts for a specified period of time, as well as publishing sample contract language in the proposed Rule. The following discussion addresses the issue of the business associate transition provisions. A discussion of the business associate sample contract language is included in Part X of the preamble.

The Department proposed 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. The additional transition period would be available to a covered entity, other than a small health plan, if, prior to the effective date of the transition provision, the covered entity had an existing contract or other written arrangement with a business associate, and such contract or arrangement was not renewed or modified between the effective date of this provision and the Privacy Rule's compliance date of April 14, 2003. The proposed provisions were intended to allow those covered entities with contracts that qualified 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 proposed to deem such contracts to be compliant with the Privacy Rule until either the covered entity had renewed or modified the contract following the compliance date of the Privacy Rule (April 14, 2003), or April 14, 2004, whichever was sooner. In cases where a contract simply renewed automatically without any change in terms or other action by the parties (also known as ''evergreen contracts''), the Department intended that such evergreen contracts would be eligible for the extension and that deemed compliance would not terminate when these contracts automatically rolled over.

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, the proposed transition provisions would not apply to small health plans, as defined in the Privacy Rule. Small health plans would be required to have all business associate contracts be in compliance with the Privacy Rule's applicable provisions, by the compliance deadline of April 14, 2004, for such covered entities.

In proposed § 164.532(e)(2), the Department provided that the new transition 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, 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 a business associate, or receive an accounting of disclosures by a business associate, as provided for by the Privacy Rule's requirements at §§ 164.524, 164.526, and 164.528. Covered entities still would 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 would have to ensure, in whatever manner effective, the appropriate cooperation by their business associates in meeting these requirements.

The Department did not propose modifications to 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.

Overview of Public Comments. The following discussion provides an overview of the public comment received on this proposal. Additional comments received on this issue are discussed below in the section entitled, ''Response to Other Public Comments.''

Most commenters on this issue expressed general support for a transition period for business associate contracts. Of these commenters, however, many requested that the Department modify the proposal in a number of different ways. For example, a number of commenters urged the Department to modify which contracts qualify for the transition period, such as by making the transition period available to contracts existing as of the compliance date of the Privacy Rule, rather than as of the effective date of the transition modification. Others requested that the Department apply the transition period to all business associate arrangements, even those arrangements for which there was no existing written contract.

Some commenters urged the Department to modify the end date of the transition period. A few of these commenters requested that the transition period apply to existing business associate contracts until they expired or were renewed, with no specified end date in the regulation. It was also suggested that the Department simply provide one extra year, until April 14, 2004, for compliance with the business associate contract provisions, without the provision that a renewal or modification of the contract would trigger an earlier transition period end date. A few commenters requested further guidance as to the types of actions the Department would or would not consider to be a ''renewal or modification'' of the contract.

Additionally, numerous commenters requested that the Department further clarify a covered entity's responsibilities with regard to their business associates during the transition period. Commenters expressed concerns with the proposal's requirement that the transition provisions would not have relieved 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 disclosures by a business associate. Similarly, commenters raised concerns that the transition provisions would not have relieved a covered entity of its responsibilities to make information available to the Secretary, including information held by a business associate, as necessary for the Secretary to determine compliance. Commenters also expressed concerns about the fact that it appeared that covered entities still would have been required to obtain satisfactory assurances from a business associate that protected health information not be used improperly by the business associate, or that the covered entity still would have been required to mitigate any known harmful effects of a business associate's improper use or disclosure of protected health information during the transition period. It was stated that cooperation by a business associate with respect to the covered entity's obligations under the Rule would be difficult, if not

impossible, to secure without a formal agreement.

A few commenters opposed the proposal, one of whom raised concerns that the proposed transition period would encourage covered entities to enter into ''stop gap'' contracts instead of compliant business associate contracts. This commenter urged that the Department maintain the original compliance date for business associate contracts.

Final Modifications. In the final Rule, the Department adopts the transition period for certain business associate contracts as proposed in the NPRM. The final Rule's transition provisions at § 164.532(d) and (e) permit 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. The transition period is available to covered entities who have an existing contract (or other written arrangement) with a business associate prior to the effective date of this modification, provided that the contract is not renewed or modified prior to the April 14, 2003, compliance date of the Privacy Rule. (See the ''Dates'' section above for the effective date of this modification.) Covered entities with contracts that qualify are permitted to continue to operate under those contracts with their business associates until April 14, 2004, or until the contract is renewed or modified, whichever is sooner. During the transition period, such contracts are deemed to be compliant with the Privacy Rule regardless of whether the contract meets the Rule's applicable contract requirements at §§ 164.502(e) and 164.504(e).

The transition provisions are intended to address the concerns of covered entities that the two-year period between the effective date and compliance date of the Privacy Rule is insufficient to reopen and renegotiate all existing contracts for the purposes of bringing them into compliance with the Rule. These provisions also provide covered entities with added flexibility to incorporate the business associate contract requirements at the time they would otherwise modify or renew the existing contract.

Given the intended purpose of these provisions, the Department is not persuaded by the comments that it is necessary to modify the provision to make the transition period available to those contracts existing prior to the Rule's compliance date of April 14, 2003, rather than the effective date of the modification, or, even less so, to any business associate arrangement regardless of whether a written contract currently exists.

A covered entity that does not have a written contract with a business associate prior to the effective date of this modification does not encounter the same burdens described by other commenters associated with having to reopen and renegotiate many existing contracts at once. The Department believes that such a covered entity should be able to enter into a compliant business associate contract by the compliance date of the Rule. Further, those covered entities whose business associate contracts come up for renewal or modification prior to the compliance date have the opportunity to bring such contracts into compliance by April 14, 2003. Thus, a covered entity that enters into a business associate contract after the effective date of this modification, or that has a contract that is renewed or modified prior to the compliance date of the Rule, is not eligible for the transition period and is required to have a business associate contract in place that meets the applicable requirements of §§ 164.502(e) and 164.504(e) by the Privacy Rule's compliance date of April 14, 2003. Further, as in the proposed Rule, the transition provisions apply only to written contracts or other written arrangements. Oral contracts or other arrangements are not eligible for the transition period. The Department clarifies, however, that nothing in these provisions requires a covered entity to come into compliance with the business associate contract provisions prior to April 14, 2003.

Similarly, in response to those commenters who requested that the Department permit existing contracts to be transitioned until April 14, 2004, regardless of whether such contracts are renewed or modified prior to that date, the Department considers a renewal or modification of the contract to be an appropriate, less burdensome opportunity to bring such contracts into compliance with the Privacy Rule. The Department, therefore, does not modify the proposal in such a way. Further, in response to commenters who requested that the Rule grandfather in existing business associate contracts until they expire or are renewed, with no specified end date in the regulation, the Department believes that limiting the transition period to one year beyond the Rule's compliance date is the proper balance between individuals' privacy interests and alleviating burden on the covered entity. All existing business associate contracts must be compliant with the Rule's business associate contract provisions by April 14, 2004.

As in the proposal, evergreen or other contracts that renew automatically without any change in terms or other action by the parties and that exist by the effective date of this modification are eligible for the transition period. The automatic renewal of such contracts itself does not terminate qualification for, or deemed compliance during, the transition period. Renewal or modification for the purposes of these transition provisions requires action by the parties involved. For example, the Department does not consider an automatic inflation adjustment to the price of a contract to be a renewal or modification for purposes of these provisions. Such an adjustment will not trigger the end of the transition period, nor make the contract ineligible for the transition period if the adjustment occurs before the compliance date of the Rule.

The transition provisions do not apply to ''small health plans,'' as defined at § 160.103. Small health plans are required to have business associate contracts that are compliant with §§ 164.502(e) and 164.504(e) by the April 14, 2004, compliance date for such entities. As explained in the proposal, the Department believes that the additional year provided by the statute for these entities to comply with the Privacy Rule provides sufficient time for compliance with the Rule's business associate provisions. In addition, the sample contract provisions provided in 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.

Like the proposal, the final Rule at § 164.532(e)(2) provides that, during the transition period, covered entities are not relieved of their responsibilities to make information available to the Secretary, including information held by a business associate, as necessary for the Secretary to determine compliance by the covered entity. Similarly, the transition period does 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 a business associate, or receive an accounting of disclosures by a business associate, as provided for by the Privacy Rule's requirements at §§ 164.524, 164.526, and 164.528. In addition, unlike the proposed Rule, the final Rule at § 164.532(e)(3) explicitly provides that with respect to those business associate contracts that qualify for the transition period as described above, a covered entity is not relieved of its obligation

under § 164.530(f) to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information by its business associate in violation of the covered entity's policies and procedures or the requirements of this subpart, as required by § 164.530(f).

The Department does not believe that a covered entity should be relieved during the transition period of its responsibilities with respect to cooperating with the Secretary or fulfilling an individual's rights with respect to protected health information held by the business associate, or mitigating any harmful effects of an inappropriate use or disclosure by the business associate. The transition period is intended to alleviate some of the burden on covered entities, but not at the expense of individuals' privacy rights. Eliminating these privacy protections and rights would severely weaken the Rule with respect to those covered entities with contracts that qualify for the transition period.

Further, the Rule provides covered entities some discretion in implementing these requirements with respect to their business associates. For example, a covered entity does not need to provide an individual with access to protected health information held by a business associate if the only information the business associate holds is a duplicate of what the covered entity maintains and to which it has provided the individual access. Covered entities are required to ensure, in whatever manner deemed effective by the covered entity, the appropriate cooperation by their business associates in meeting these requirements.

In response to other concerns from commenters, the Department clarifies that a covered entity is not required to obtain satisfactory assurances (in any form), as required by § 164.502(e)(1), from a business associate to which the transition period applies. The transition period effectively deems such qualified contracts to fulfill the requirement for satisfactory assurances from the business associate.

The Department is aware that the transition provisions may encourage some covered entities to enter into contracts before the effective date of the modification solely to take advantage of the transition period, rather than encourage such entities to execute fully compliant business associate contracts. However, the Department believes that the provision appropriately limits the potential for such misuse by requiring that qualified contracts exist prior to the modification effective date rather than the Privacy Rule's compliance date. Further, the transition provisions do not relieve the covered entity of its obligations with respect to protected health information held by the business associate and, therefore, ensures that an individual's rights, as provided for by the Rule, remain intact during the transition period.

Response to Other Public Comments

Comment: One commenter requested that the transition period also be applied to the requirement that a group health plan amend plan documents pursuant to § 164.504(f) before protected health information may be disclosed to the plan sponsor.

Response: The Department does not make such a modification. The intent of the business associate transition provisions is to alleviate burden on those covered entities with many existing contracts, where as a result, the two-year period between the effective date and compliance date of the Privacy Rule may be insufficient to reopen and renegotiate all such contracts for the purposes of bringing them into compliance with the Rule. The Privacy Rule does not require a business associate contract for disclosure of protected health information from a group health plan to a plan sponsor. Rather, the Rule permits a group health plan to disclose protected health information to a plan sponsor if, among other requirements, the plan documents are amended to appropriately reflect and restrict the plan sponsor's uses and disclosures of such information. As the group health plan should only have one set of plan documents that must be amended, the same burdens described above do not exist with respect to this activity. Thus, the Department expects that group health plans will be able to modify plan documents in accordance with the Rule by the Rule's compliance date.

Comment: Many commenters continued to recommend various modifications to the business associate standard, unrelated to the proposed modifications. For example, some commenters urged that the Department eliminate the business associate requirements entirely. Several commenters urged that the Department exempt covered entities from having to enter into contracts with business associates who are also covered entities under the Privacy Rule. Alternatively, one commenter suggested that the Department simplify the requirements by requiring a covered entity that is a business associate to specify in writing the uses and disclosures the covered entity is permitted to make as a business associate.

Other commenters requested that the Department allow business associates to self-certify or be certified by a third party or HHS as compliant with the Privacy Rule, as an alternative to the business associate contract requirement.

Certain commenters urged the Department to modify the Rule to eliminate the need for a contract with accreditation organizations. Some commenters suggested that the Department do so by reclassifying private accreditation organizations acting under authority from a government agency as health oversight organizations, rather than as business associates.

Response: The proposed modifications regarding business associates were intended to address the concerns of commenters with respect to having insufficient time to reopen and renegotiate what could be thousands of contracts for some covered entities by the compliance date of the Privacy Rule. The proposed modifications did not address changes to the definition of, or requirements for, business associates generally. The Department has, in previous guidance, as well as in the preamble to the December 2000 Privacy Rule, explained its position with respect to most of the above concerns. However, the Department summarizes its position in response to such comments briefly below.

The Department recognizes that most covered entities acquire the services of a variety of other persons or entities to assist in carrying covered entities' health care activities. The business associate provisions are necessary to ensure that individually identifiable health information created or shared in the course of these relationships is protected. Further, without the business associate provisions, covered entities would be able to circumvent the requirements of the Privacy Rule simply by contracting out certain of its functions.

With respect to a contract between a covered entity and a business associate who is also a covered entity, the Department restates its position that a covered entity that is a business associate should be restricted from using or disclosing the protected health information it creates or receives as a business associate for any purposes other than those explicitly provided for in its contract. Further, to modify the provisions to require or permit a type of written assurance, other than a contract, by a covered entity would add unnecessary complexity to the Rule.

Additionally, the Department at this time does not believe that a business associate certification process would

provide the same kind of protections and guarantees with respect to a business associate's actions that are available to a covered entity through a contract under State law. With respect to certification by a third party, it is unclear whether such a process would allow for any meaningful enforcement (such as termination of a contract) for the actions of a business associate. Further, the Department could not require that a business associate be certified by a third party. Thus, the Privacy Rule still would have to allow for a contract between a covered entity and a business associate.

The Privacy Rule explicitly defines organizations that accredit covered entities as business associates. See the definition of ''business associate'' at § 160.103. The Department defined such organizations as business associates because, like other business associates, they provide a service to the covered entity during which much protected health information is shared. The Privacy Rule treats all organizations that provide accreditation services to covered entities alike. The Department has not been persuaded by the comments that those accreditation organizations acting under grant of authority from a government agency should be treated differently under the Rule and relieved of the conditions placed on other such relationships. However, the Department understands concerns regarding the burdens associated with the business associate contract requirements. The Department clarifies that the business associate provisions may be satisfied by standard or model contract forms which could require little or no modification for each covered entity. As an alternative to the business associate contract, these final modifications permit a covered entity to disclose a limited data set of protected health information, not including direct identifiers, for accreditation and other health care operations purposes subject to a data use agreement. *See* § 164.514(e).

Comment: A number of commenters continued to express concern over a covered entity's perceived liability with respect to the actions of its business associate. Some commenters requested further clarification that a covered entity is not responsible for or required to monitor the actions of its business associates. It also was suggested that such language expressly be included in the Rule's regulatory text. One commenter recommended that the Rule provide that business associates are directly liable for their own failure to comply with the Privacy Rule. Another commenter urged that the Department eliminate a covered entity's obligation to mitigate any harmful effects caused by a business associate's improper use or disclosure of protected health information.

Response: The Privacy Rule does not require a covered entity to actively monitor the actions of its business associates nor is the covered entity responsible or liable for the actions of its business associates. Rather, the 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 obligations under the contract, the covered entity take steps to cure the breach or end the violation. *See* § 164.504(e)(1). The Department does not believe a regulatory modification is necessary in this area. The Department does not have the statutory authority to hold business associates, that are not also covered entities, liable under the Privacy Rule.

With respect to mitigation, the Department does not accept the commenter's suggestion. When protected health information is used or disclosed inappropriately, the harm to the individual is the same, regardless of whether the violation was caused by the covered entity or a by business associate. Further, this provision is not an absolute standard intended to require active monitoring of the business associate or mitigation of all harm caused by the business associate. Rather, the provision applies only if the covered entity has actual knowledge of the harm, and requires mitigation only ''to the extent practicable'' by the covered entity. *See* § 164.530(f).

Comment: Several commenters asked the Department to provide additional clarification as to who is and is not a business associate for purposes of the Rule. For example, commenters questioned whether researchers were business associates. Other commenters requested further clarification as to when a health care provider would be the business associate of another health care provider. One commenter asked the Department to clarify whether covered entities that engage in joint activities under an organized health care arrangement (OHCA) are required to have a business associate contract. Several commenters asked the Department to clarify that a business associate agreement is not required with organizations or persons where contact with protected health information would result inadvertently (if at all), for example, janitorial services.

Response: The Department provides the following guidance in response to commenters. Disclosures from a covered entity to a researcher for research purposes as permitted by the Rule do not require a business associate contract. This remains true even in those instances where the covered entity has hired the researcher to perform research on the covered entity's own behalf because research is not a covered function or activity. However, the Rule does not prohibit a covered entity from entering into a business associate contract with a researcher if the covered entity wishes to do so. Notwithstanding the above, a covered entity must enter into a data use agreement, as required by § 164.514(e), prior to disclosing a limited data set for research purposes to a researcher.

With respect to business associate contracts between health care providers, the Privacy Rule explicitly excepts from the business associate requirements disclosures by a covered entity to a health care provider for treatment purposes. *See* § 164.502(e)(1). Therefore, any covered health care provider (or other covered entity) may share protected health information with a health care provider for treatment purposes without a business associate contract. The Department does not intend the Rule to interfere with the sharing of information among health care providers for treatment. However, this exception does not preclude one health care provider from establishing a business associate relationship with another health care provider for some other purpose. For example, a hospital may enlist the services of another health care provider to assist in the hospital's training of medical students. In this case, a business associate contract would be required before the hospital could allow the health care provider access to patient health information.

As to disclosures among covered entities who participate in an organized health care arrangement, the Department clarifies that no business associate contract is needed to the extent the disclosure relates to the joint activities of the OHCA.

The Department also clarifies that a business associate contract is not required with persons or organizations whose functions, activities, or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be de minimus, if at all. For example, a health care provider is not required to enter into a business associate contract with its janitorial service because the performance of such service does not involve the use or disclosure of protected health information. In this case, where a janitor has contact with

protected health information incidentally, such disclosure is permissible under § 164.502(a)(1)(iii) provided reasonable safeguards are in place.

The Department is aware that similar questions still remain with respect to the business associate provisions of the Privacy Rule and intends to provide technical assistance and further clarifications as necessary to address these questions.

Comment: A few commenters urged that the Department modify the Privacy Rule's requirement for a covered entity to take reasonable steps to cure a breach or end a violation of its business associate contract by a business associate. One commenter recommended that the requirement be modified instead to require a covered entity who has knowledge of a breach to ask its business associate to cure the breach or end the violation. Another commenter argued that a covered entity only should be required to take reasonable steps to cure a breach or end a violation if the business associate or a patient reports to the privacy officer or other responsible employee of the covered entity that a misuse of protected health information has occurred.

Response: It is expected that a covered entity with evidence of a violation will ask its business associate, where appropriate, to cure the breach or end the violation. Further, the Department intends that whether a covered entity ''knew'' of a pattern or practice of the business associate in breach or violation of the contract will be consistent with common principles of law that dictate when knowledge can be attributed to a corporate entity. Regardless, a covered entity's training of its workforce, as required by § 164.530(b), should address the recognition and reporting of violations to the appropriate responsible persons with the entity.

Comment: Several commenters requested clarification as to whether a business associate is required to provide individuals with access to their protected health information as provided by § 164.524 or an accounting of disclosures as provided by § 164.528, or amend protected health information as required by § 164.526. Some commenters wanted clarification that the access and amendment provisions apply to the business associate only if the business associate maintains the original designated record set of the protected health information.

Response: Under the Rule, the covered entity is responsible for fulfilling all of an individual's rights, including the rights of access, amendment, and accounting, as provided for by §§ 164.524, 164.526, and 164.528. With limited exceptions, a covered entity is required to provide an individual access to his or her protected health information in a designated record set. This includes information in a designated record set of a business associate, unless the information held by the business associate merely duplicates the information maintained by the covered entity. However, the Privacy Rule does not prevent the parties from agreeing through the business associate contract that the business associate will provide access to individuals, as may be appropriate where the business associate is the only holder of the, or part of the, designated record set.

As governed by § 164.526, a covered entity must amend protected health information about an individual in a designated record set, including any designated record sets (or copies thereof) held by a business associate. Therefore, the Rule requires covered entities to specify in the business associate contract that the business associate will make protected health information available for amendment and will incorporate amendments accordingly. The covered entity itself is responsible for addressing requests from individuals for amendment and coordinating such requests with its business associate. However, the Privacy Rule also does not prevent the parties from agreeing through the contract that the business associate will receive and address requests for amendment on behalf of the covered entity.

With respect to accounting, § 164.528 requires a covered entity to provide an accounting of certain disclosures, including certain disclosures by its business associate, to the individual upon request. The business associate contract must provide that the business associate will make such information available to the covered entity in order for the covered entity to fulfill its obligation to the individual. As with access and amendment, the parties can agree through the business associate contract that the business associate will provide the accounting to individuals, as may be appropriate given the protected health information held by, and the functions of, the business associate.

Comment: One commenter asked whether a business associate agreement in electronic form, with an electronic signature, would satisfy the Privacy Rule's business associate requirements.

Response: The Privacy Rule generally allows for electronic documents to qualify as written documents for purposes of meeting the Rule's requirements. This also applies with respect to business associate agreements. However, currently, no standards exist under HIPAA for electronic signatures. Thus, in the absence of specific standards, covered entities should ensure any electronic signature used will result in a legally binding contract under applicable State or other law.

Comment: Certain commenters raised concerns with the Rule's classification of attorneys as business associates. A few of these commenters urged the Department to clarify that the Rule's requirement at § 164.504(e)(2)(ii)(H), which requires a contract to state the business associate must make information relating to the use or disclosure of protected health information available to the Secretary for purposes of determining the covered entity's compliance with the Rule, not apply to protected health information in possession of a covered entity's lawyer. Commenters argued that such a requirement threatens to impact attorney-client privilege. Others expressed concern over the requirement that the attorney, as a business associate, must return or destroy protected health information at termination of the contract. It was argued that such a requirement is inconsistent with many current obligations of legal counsel and is neither warranted nor useful.

Response: The Department does not modify the Rule in this regard. The Privacy Rule is not intended to interfere with attorney-client privilege. Nor does the Department anticipate that it will be necessary for the Secretary to have access to privileged material in order to resolve a complaint or investigate a violation of the Privacy Rule. However, the Department does not believe that it is appropriate to exempt attorneys from the business associate requirements.

With respect to the requirement for the return or destruction of protected health information, the Rule requires the return or destruction of all protected health information at termination of the contract only where feasible or permitted by law. Where such action is not feasible, the contract must state that the information will remain protected after the contract ends for as long as the information is maintained by the business associate, and that further uses and disclosures of the information will be limited to those purposes that make the return or destruction infeasible.

Comment: One commenter was concerned that the business associate provisions regarding the return or

destruction of protected health information upon termination of the business associate agreement conflict with various provisions of the Bank Secrecy Act, which require financial institutions to retain certain records for up to five years. The commenter further noted that there are many State banking regulations that require financial institutions to retain certain records for up to ten years. The commenter recommended that the Department clarify, in instances of conflict with the Privacy Rule, that financial institutions comply with Federal and State banking regulations.

Response: The Department does not believe there is a conflict between the Privacy Rule and the Bank Secrecy Act retention requirements or that the Privacy Rule would prevent a financial institution that is a business associate of a covered entity from complying with the Bank Secrecy Act. The Privacy Rule generally requires a business associate contract to provide that the business associate will return or destroy protected health information upon the termination of the contract; however, it does not require this if the return or destruction of protected health information is infeasible. Return or destruction would be considered ''infeasible'' if other law, such as the Bank Secrecy Act, requires the business associate to retain protected health information for a period of time beyond the termination of the business associate contract. The Privacy Rule would require that the business associate contract extend the protections of the contract and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible. In this case, the business associate would have to limit the use or disclosure of the protected health information to purposes of the Bank Secrecy Act or State banking regulations.

Comment: A commenter requested clarification concerning the economic impact on business associates of the cost-based copying fees allowed to be charged to individuals who request a copy of their medical record under the right of access provided by the Privacy Rule. See § 164.524. According to the commenter, many hospitals and other covered entities currently outsource their records reproduction function for fees that often include administrative costs over and above the costs of copying. In some cases, the fees may be set in accordance with State law. The Privacy Rule, at § 164.524(c)(4), however, permits only reasonable, cost-based copying fees to be charged to individuals seeking to obtain a copy of their medical record under their right of access. The commenter was concerned that others seeking copies of all or part of the medical record, such as payers, attorneys, or entities that have the individual's authorization, would try to claim the limited copying fees provided in § 164.524(c)(4). The commenter asserted that such a result would drastically alter the economics of the outsourcing industry, driving outsourcing companies out of business, and raising costs for the health industry as a whole. A clarification that the fee structure in § 164.524(c)(4) applies only to individuals exercising their right of access was sought.

Response: The Department clarifies that the Rule, at § 164.524(c)(4), limits only the fees that may be charged to individuals, or to their personal representatives in accordance with § 164.502(g), when the request is to obtain a copy of protected health information about the individual in accordance with the right of access. The fee limitations in § 164.524(c)(4) do not apply to any other permissible disclosures by the covered entity, including disclosures that are permitted for treatment, payment or health care operations, disclosures that are based on an individual's authorization that is valid under § 164.508, or other disclosures permitted without the individual's authorization as specified in § 164.512.

The fee limitation in § 164.524(c)(4) is intended to assure that the right of access provided by the Privacy Rule is available to all individuals, and not just to those who can afford to do so. Based on the clarification provided, the Department does not anticipate that this provision will cause any significant disruption in the way that covered entities do business today. To the extent hospitals and other entities outsource this function because it is less expensive than doing it themselves, the fee limitation for individuals seeking access under § 164.524 will affect only a portion of this business; and, in these cases, hospitals should still find it economical to outsource these activities, even if they can only pass on a portion of the costs to the individual.

K. Technical Corrections and Other Clarifications

1. Definition of ''Individually Identifiable Health Information''

Part 160 contains the definitions that are relevant to all of the Administrative Simplification provisions at Parts 160 through 164. Although the term ''individually identifiable health information'' is relevant to Parts 160 through 164, it is defined in § 164.501 of the Privacy Rule. To correct this technical error, the Department proposed to move the definition of individually identifiable health information from § 164.501 to § 160.103.

The limited comment on this proposal supported moving the definition into § 160.103, for the same reasons cited by the Department. Therefore, the Department in this final Rule deletes the definition of ''individually identifiable health information'' from § 164.501 of the Privacy Rule, and adds the definition to § 160.103.

2. Technical Corrections

The Privacy Rule contained some technical and typographical errors. Therefore, the Department is making 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 § 164.514(d)(5), the word ''discloses'' is corrected to read ''disclose.''

n. In § 164.520(c), in the introductory text, ''(c)(4)'' is corrected to read ''(c)(3).''

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

p. In § 164.530(i)(4)(ii)(A), in the second line, ''the requirements'' is

replaced with the word ''specifications.''

IV. Final Regulatory Impact Analysis

Federal law (5 U.S.C. 804(2), as added by section 251 of Pub. L. No. 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 adopted in this rulemaking will have an annual effect on the economy of at least $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 December 2000 preamble to 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 modifications to the Privacy Rule adopted by this 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 modifications 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 Department estimates the impact of the modifications adopted in this rulemaking will be a net reduction of costs associated with the Privacy Rule of at least $100 million over ten years.

The modifications 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, this rulemaking contains a number of changes that, though important, can be categorized as clarifications of intended policy. For example, the modifications permit certain uses and disclosures of protected health information that are incidental to an otherwise permitted use or disclosure. This change recognizes 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 adopted in this rulemaking (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. Public comments have indicated that these provisions would be interpreted in a way that could significantly increase costs. However, because that was not the intent of the December 2000 Privacy Rule, the Department is not ascribing cost savings to the clarification of these provisions.

A. Summary of Costs and Benefits in the December 2000 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 are affected by the modifications adopted in this rulemaking.

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

The modifications adopted 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.

The Department received few comments on this section of the March 2002 proposal. Most of the comments on the cost implications of the modifications indicated a general belief that the costs would be higher than the Department estimated. None of commenters, however, provided sufficient specific information concerning costs to permit the Department to adjust its estimates. The public comment on each of the key policy areas is summarized in the following sections. However, the estimated cost impact of each area has not changed.

1. Consent

Under the December 2000 Privacy Rule, a covered health care provider with a direct treatment relationship with an individual must have obtained 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 have obtained such a consent if they so chose. The initial cost of the consent requirement was estimated in December 2000 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 modifications 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

[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.

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.D.1. above, the Department received many comments supporting the proposed elimination of the consent requirement on the ground that it created 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 over a ten-year period were $103 million, the comments suggest that the costs would likely 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 over a ten-year period.

Response to Public Comments

Comment: As discussed in section III.H. above, many commenters expressed support for the proposed requirement that certain health care providers make a good faith effort to obtain a written acknowledgment of receipt of the notice, as a workable alternative to the Rule's prior consent requirement. Many of these commenters conveyed support for the flexibility of the requirement, and most commenters agreed that eliminating the consent requirement would mean considerable savings.

Response: The Department received no public comment containing empirical, direct evidence on the estimates of financial impact that either supported or contradicted the Department's calculations. Therefore, our estimates remain unchanged.

Comment: Many other commenters confused the net savings associated with the Administrative Simplification provisions with cost savings associated with the Privacy Rule, and relied on this misinformation to argue in favor of retaining the consent provisions for treatment, payment, and health care operations.

Response: These commenters were essentially propounding a policy choice and not making a comment on the validity of the estimates for cost savings associated with the elimination of the consent requirement. The comments did not include any reliable estimation that would cause the Department to reevaluate its savings estimate.

2. Notice

In eliminating the consent requirement, the Department preserves 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 do not change this distribution requirement, but add a new documentation requirement. A covered health care provider with a direct treatment relationship is 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 is required. Since the modification does 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.

However, the additional effort by direct treatment providers in obtaining and documenting the individual's acknowledgment of receipt of the notice adds costs. This new requirement attaches only to the initial provision of notice by a direct treatment provider to an individual after the compliance date. Under the modification, providers have considerable flexibility on how to achieve this. Some providers could 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 its December 2000 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 modification to the notice requirement provides greater flexibility and, therefore, greater opportunity to reduce costs compared to the consent requirement. Without knowing exactly how direct treatment providers will decide to exercise the flexibility provided, the Department cannot, with any precision, estimate the cost to implement this provision. In the NPRM, the Department estimated that the flexibility of the notice acknowledgment requirement would mean that the cost of the notice acknowledgment would be 20 percent less than the cost of the signed consent. The Department did not receive any comments on this estimate and, therefore, does not change it's estimate that the additional cost of the signature requirement, on average, is $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 to which the new good faith acknowledgment requirement will attach. 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 will be $24 million and the total cost over ten years will be $184 million.

Response to Public Comments

Comment: As discussed in section III.H. above, a number of other commenters expressed concern over the administrative and financial burden the requirement to obtain a good faith acknowledgment of the notice would impose.

Response: The Department received no public comment containing empirical, direct evidence on the estimates of financial impact that either supported or contradicted the Department's calculations. Therefore, our estimates remain unchanged.

Comment: One commenter requested that model language for the notice be developed as a means of reducing the costs associated with Privacy Rule compliance.

Response: As stated in section III.H. above, in the final Rule, the Department sought to retain the maximum flexibility by requiring only that the acknowledgment be in writing and does not prescribe other details of the form

that the acknowledgment must take or the process for obtaining the acknowledgment. This permits covered health care providers the discretion to design the acknowledgment process as best suited to their practices, including the option of obtaining an electronic acknowledgment regardless of whether the notice is provided electronically or on paper. Furthermore, there is no change to the substance of the notice and the commenter provided no empirical, direct benefit/cost data in support of their proposal.

Comment: The Department received comments expressing opposition to obtaining written acknowledgment of the receipt of the notice because it is too costly. Others commented that the acknowledgment increases the administrative burden as it would not replace a signed consent for uses and disclosures of health information when State law requires providers to obtain consent.

Response: The Department received no public comment containing empirical, direct evidence on the estimates of financial impact that either supported or contradicted the Department's calculations. Therefore, our estimates remain unchanged.

Comment: A number of commenters expressed concern over the perceived increase in liability that would arise from the discretionary standard of ''good faith'' efforts (i.e., risk of tort-based litigation for private right of action under State laws).

Response: The Department received no estimate of the impact of this perceived risk of liability. As no empirical, direct evidence on the estimates of financial impact that either supported or contradicted the Department's calculations was supplied, our estimates remain unchanged.

3. Business Associates

The Privacy Rule requires a covered entity to have a written contract, or other arrangement, that documents satisfactory assurances that a business associates 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 modification adopted 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, the Department includes sample business associate contract language as part of the preamble to this rulemaking. This sample language is only suggested language and is not a complete contract. The sample 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. Certain provisions of the sample language have been revised, as described in more detail below, based on the public comment received on the proposal. The December 2000 regulatory impact analysis assumed the development of such standard language by trade and professional associations. While this has occurred to some degree, the Department received strong public comment supporting the for sample contract language. The Department expects that trade and professional associations will continue to provide assistance to their members. However, the sample contract language in this rulemaking 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 changes being adopted to the sample contract language do not affect these cost estimates.

The Department, in this rulemaking, also gives most covered entities additional time to conform written contracts to the privacy standards. Under the modification, a covered entity's written business associate contracts, existing at the time the modifications become effective, are 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 is 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 the average delay that will occur. Therefore, the Department is uncertain about the extent of the cost savings attributable to this modification.

Response to Public Comments

Comment: While many commenters supported the business associate transition provisions as helpful to reducing the administrative burden and cost of compliance, commenters argued that the business associate provisions would still be very burdensome and costly to implement, especially for small and solo businesses.

Response: The Department acknowledges that there are compliance costs associated with the business associate standards. However, no commenters supplied empirical, direct evidence in support of or contradictory to the Department's estimates of the cost savings associated with the business associate transition provisions. Therefore, our estimates remain unchanged.

Comment: Some commenters disputed the estimated costs of complying with the business associate requirements based on the quantity of contracts (with suppliers, physicians, local agencies and national concerns), and the number of hours necessary to individually tailor and renegotiate all of these contracts.

Response: These comments address the underlying costs of the business associate requirements and do not address the reduction in costs afforded through the sample business associate agreement language. Moreover, no empirical, direct evidence, based on accomplished workload rather than extrapolations of singular events, were provided to contradict the Department's calculations. Therefore, our estimates remain unchanged.

4. Marketing

Under § 164.514(e) of the December 2000 Privacy Rule, certain health-related communications were subject to special conditions on marketing communications, if they also served to promote the use or sale of a product or service. These marketing conditions required that particular disclosures be made as part of the marketing materials sent to individuals. Absent these disclosures, protected health information could 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 created a potential burden on covered entities to make difficult assessments regarding many of their communications. The modifications to the marketing provisions relieve the burden on covered entities by making most marketing subject to an authorization requirement (*see* § 164.508(a)(3)), making clear that necessary treatment and health care operations activities were not marketing, and eliminating the § 164.514(e) conditions on marketing communications.

In developing the December 2000 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 modifications 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 modifications is to lower the costs associated with the Privacy Rule.

Response to Public Comment

Comment: Many providers, especially mental health providers, opposed the changes to marketing and consent as they fear increased access to individually identifiable health information would cause patients to refrain from seeking treatment. By not seeking timely treatment, the medical conditions could worsen, and result in increased or additional costs to society.

Response: The commenters did not attempt to segment out the cost attributed to marketing alone. In fact, no empirical, direct evidence on the estimates of financial impact that either supported or contradicted the Department's calculations was provided. Therefore, our estimates remain unchanged.

5. Research

In the final impact analysis of the December 2000 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 modifications simplify and reduce the number of criteria required for an IRB or Privacy Board to approve a waiver of authorization to better conform to the Common Rule's waiver criteria for informed consent to participate in the research study. The Department estimates that the net effect of these modifications is to reduce the time necessary to assemble the 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 December 2000 Privacy Rule. Although the Department requested information to better assess this cost savings, the public comment period failed to produce any sound data. Therefore, the Department's estimates have not changed.

The Department adopts three other modifications to simplify the Privacy Rule requirements to relieve the potential administrative burden on research. First, the modifications permit a covered entity to use and disclose protected health information in the form of a limited data set for research, public health, and health care operations. A limited data set does not contain any direct identifiers of individuals, but may contain any other demographic or health information needed for research, public health or health care operations purposes. The covered entity must obtain a data use agreement from the recipient of a limited data set pursuant to which the recipient agrees to restrict use and disclosure of the limited data set and not to identify or contact any individual. With a data use agreement, a researcher may access a limited data set without obtaining individual authorization or having to go through an IRB or a Privacy Board for a waiver of the authorization. (*See* discussion at III.G.2.) Second, the modifications simplify the accounting procedures for research disclosures by the covered entity by eliminating the need to account for disclosures which the individual has authorized or which are part of a limited data set, and by providing a simplified basis to account for a research disclosure involving 50 or more records. (*See* discussion at III.F.2.) Third, the modifications simplify the authorization process for research to facilitate the combining of the informed consent for participation in the research itself with an authorization required under the Privacy Rule. (*See* discussion at III.E.2.) Any cost savings attributed to the later two modifications would accrue primarily to the covered entity disclosing protected health information for research purposes and, therefore, would not affect the costs estimated here for the impact of the Privacy Rule on IRBs.

With regard to limited data sets, the Department anticipates that the modification will avoid IRBs having to review and approve researchers' requests for waiver of authorization for numerous studies that are undertaken today without IRB review and approval. For example, a researcher may not need IRB approval or waiver of informed consent to collect health information that is linked to the individual only by inclusion of the individual's zip code as this may not be personally identifying information under the Common Rule. However, this information would not be considered de-identified information under the Privacy Rule and it could not be disclosed to the researcher without the individual's authorization or an IRB waiver of that authorization. With the limited data set, research that does not require direct identifiers can continue to go on expeditiously without adding burden to IRBs and Privacy Boards. Similarly, limited data sets, similar to the Hospital Discharge Abstract data, will permit much useful information to be available for research, public health, and health care operations purposes.

Although there was broad support for limited data sets in the comments received by the Department, we do not have sufficient information to estimate the amount of research that currently occurs without IRB review or approval and which, but for the provision on limited data sets, would have had to involved the IRB to meet the use and disclosure requirements of the Privacy Rule. Nor did the comments supply information upon which the Department could reasonably rely in making a estimate of the cost savings. Therefore, the Department does not increase its

estimated savings for research to reflect this modification, although we are confident that the overall impact of the Privacy Rule on research will be much lower based on the modifications adopted in this rulemaking.

Response to Public Comments

Comment: The Department received a number of comments that argued that the Privacy Rule would increase costs and workloads for researchers and research institutions. One commenter delineated these issues as: (1) An increased difficulty in recruiting research participants; (2) the need for increased IRB scrutiny (and the associated resource costs); and (3) the additional paperwork and documentation required.

Response: The Department recognized the impact of the final Privacy Rule on researchers and research institutions and provided a cost estimate for this impact as part of the Final Rule. Likewise, the NPRM offered modifications, such as more closely aligning the Privacy and Common Rule criteria, to ease the burden and, correspondingly, estimated cost savings of these proposed modifications. The specific comments appear to dispute the research cost estimates in the final Rule, as their delineated issues are not reflective of the modifications and cost savings specified in the NPRM. In any event, no reliable empirical, direct information on the estimates of financial impact that either supported or contradicted the Department's calculations was provided. Therefore, our estimates remain unchanged.

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 modifications adopted 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 at least partially offset by the savings in the elimination of the consent. As discussed above, to the extent concerns 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 sample 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 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 modifications 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 concerns 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 sample 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 modifications.

E. Benefits

The benefits of various provisions of these modifications will be strong privacy protections for individuals coupled with increased access to quality health care, and ease of compliance with privacy protections by covered entities. The changes will have the benefit of eliminating obstacles that could interfere with patient access to timely and high quality health care. The modifications will also improve quality health care by removing obstacles that may have interfered with research activities that form the basis of advancements in medical technology and provide greater understanding of disease. It is extremely difficult to quantify the benefits of enhanced privacy of medical records and elimination of obstacles to research and quality activities. This section provides examples of the qualitative benefits of these Privacy Rule modifications.

1. Strengthened Notice, Flexible Consent

The new requirement that a covered entity make a good faith attempt to obtain written acknowledgment of the notice of privacy practices will increase privacy protections to patients. The strengthened notice requirement will focus individuals on uses and disclosures of their health information, and assure that individuals have the opportunity to discuss privacy concerns with the health care providers with whom they have direct treatment relationships. Awareness of privacy practices should provide patients with a greater degree of comfort in discussing sensitive personal information with

their doctors. The strengthened notice standard was adopted in tandem with changes to make consent more flexible. The changes to the consent requirement have the benefit of removing significant barriers to health care. In many circumstances, the consent requirement would have resulted in delayed treatment and, in other circumstances, would have required patients to be greatly inconvenienced at a time when they needed care, by forcing additional trips simply to sign consent forms. These modifications have the benefit of removing barriers to access to health care that would have resulted from the consent requirement while preserving important privacy protections in the notice standard.

2. Research

Research is key to the continued availability of high quality health care. The modifications remove potential barriers to research. For example, the modifications streamline the criteria to be used by IRBs or Privacy Boards in approving a waiver of individual authorization for research that could not otherwise be done and ensure the criteria are compatible with similar waiver determinations under the Common Rule. Thus, administrative burdens on IRBs and Privacy Boards are eased, without diminishing the health information privacy and confidentiality standards for research. In addition, the research transition provisions have been modified to ensure that the Privacy Rule does not interfere with ongoing or future research for which an individual has granted permission to use his information. By permitting this research to continue, these modifications make sure that vast research resources continue to be usable for important research that result in development of new medical technology and increased quality of health care.

3. Sharing Information for Quality Activities and Public Health

Health plans and health care providers play a valuable role in assessing the quality of health care and improving health care outcomes. The modifications ensure access to health information needed by covered entities and others involved in quality activities. The increased sharing of information will help to limit medical error rates and to determine appropriate, high quality treatment for specific conditions by encouraging these issues to be studied and allowing benchmarking against similar entities. The modifications, in creating a limited data set, also encourages private entities to continue studies and research in support of public health activities. These activities help reduce the spread and occurrence of diseases.

4. Availability of Information About Treatment Alternatives

Understanding treatment alternatives is an important factor in increasing an individual's involvement in his or her own treatment and making informed health care decisions. By streamlining the marketing requirements, the modifications make it easier for a covered entity to understand that they may share valuable information about treatment alternatives with their patients or enrollees, and the conditions for doing so. These modifications make sure that covered entities will be permitted to continue to share important treatment alternative information that gives patients knowledge about newer, less expensive, and/or more appropriate health care options.

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 rulemaking. The Department examined a number of alternatives to these modifications. 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 final 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 December 2000 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 Final Regulatory Impact Analysis, above, the net affect of the modifications 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 30-day notice in the **Federal Register** and solicit public comment before a collection of information requirement is submitted to the Office of Management and Budget (OMB) for review and approval. In order to fairly evaluate whether an information collection should be approved by OMB, section 3506(c)(2)(A) of the PRA requires that 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; and
- Recommendations to minimize the information collection burden on the affected public, including automated collection techniques.

Section A below summarizes the proposed information collection requirements on which we explicitly seek, and will consider, public comment for 30 days. Due to the complexity of this regulation, and to avoid redundancy of effort, we are referring readers to Section V (Final Regulatory Impact Analysis published in the **Federal Register** on December 28, 2000), to review the detailed cost assumptions associated with these PRA requirements.

Section B below references the HIPAA Privacy Rule regulation sections published for 60-day public comment on November 3, 1999, and for 30-day public comment on December 28, 2000,

in compliance with the PRA public comment process. These earlier publications contained the information collection requirements for these sections as required by the PRA. The portions of the Privacy Rule, included by reference only in Section B, have not changed subsequent to the two public comment periods. Thus, the Department has fulfilled its statutory obligation to solicit public comment on the information collection requirements for these provisions. The information in Section B is pending OMB PRA approval, but is not reopened for comment. However, for clarity purposes, we will upon this publication submit to OMB for PRA review and approval the entire set of information collection requirements required referenced in §§ 160.204, 160.306, 160.310, 164.502, 164.504, 164.506, 164.508, 164.510, 164.512, 164.514, 164.520, 164.522, 164.524, 164.526, 164.528, and 164.530.

Section A

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

Under the Privacy Rule, as issued in December 2000, a covered health care provider that has a direct treatment relationship with individuals would have had, except in certain circumstances, to obtain an individual's consent to use or disclose protected health information to carry out treatment, payment, and health care operations. The amended final Rule eliminates this requirement.

2. Section 164.520—Notice of Privacy Practices for Protected Health Information

The amended final Privacy Rule imposes a good faith effort on direct treatment providers to obtain an individual's acknowledgment of receipt of the entity's 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.

The underlying requirements for notice of privacy practices for protected health information are not changed. These requirements provide that, except in certain circumstances set forth in this section of the Rule, individuals have a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information. To comply with this requirement a covered entity must provide a notice, written in plain language, that includes the elements set forth at § 164.520(b). For health plans, there will be an average of 160.2 million notices each year. We assume that the most efficient means of distribution for health plans will be to send them out annually as part of the materials they send to current and potential enrollees, even though it is not required by the regulation. The number of notices per health plan per year would be about 10,570. We further estimate that it will require each health plan, on average, only 10 seconds to disseminate each notice. The total annual burden associated with this requirement is calculated to be 267,000 hours.

Health care providers with direct treatment relationships would:

- Provide a copy of the notice to an individual at the time of first service delivery to the individual;
- Make the notice available at the service delivery site for individuals to request and take with them;
- Whenever the content of the notice is revised, make it available upon request and post it, if required by this section, in a location where it is reasonable to expect individuals seeking services from the provider to be able to read the notice.

The annual number of notices disseminated by all providers is 613 million. We further estimate that it will require each health care provider, on average, 10 seconds to disseminate each notice. This estimate is based upon the assumption that the required notice will be incorporated into and disseminated with other patient materials. The total annual burden associated with this requirement is calculated to be 1 million hours. However, the amended final Privacy Rule also imposes a good faith effort on direct treatment providers to obtain an individual's acknowledgment of receipt of the provider's notice, and to document such acknowledgment or, in the absence of such acknowledgment, the provider's good faith efforts to obtain it. The estimated burden for the acknowledgment of receipt of the notice is 10 seconds for each notice. This is based on the fact that the provider does not need to take elaborate steps to receive acknowledgment. Initialing a box on an existing form or some other simple means will suffice. With the annual estimate of 613,000,000 acknowledgment forms it is estimated that the acknowledgment burden is 1,000,000 hours.

A covered entity is also required to document compliance with the notice requirements by retaining copies of the versions of the notice issued by the covered entity, and a direct treatment provider is required to retain a copy of each individual's acknowledgment or documentation of the good faith effort as required by § 164.530(j).

3. Appendix to Preamble—Sample Business Associate Contract Provisions

The Department also solicits public comments on the collection of information requirements associated with the model business associate contract language displayed in the Appendix to this preamble Rule. The language displayed has been changed in response to comments on the language that was published with the Notice of Proposed Rulemaking on March 27, 2002. The Department provided the model business associate contract provisions in response to numerous requests for guidance. These provisions were 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 B

As referenced above, the Department has complied with the public comment process as it relates to the information collection requirements contained in the sections of regulation referenced below. The Department is referencing this information solely for the purposes of providing an overview of the regulation sections containing information collection requirements established by the final Privacy Rule.

Section 160.204—Process for Requesting Exception Determinations
Section 160.306—Complaints to the Secretary
Section 160.310—Responsibilities of Covered Entities
Section 164.502—Uses and Disclosures of Protected Health Information: General Rules
Section 164.504—Uses and Disclosures—Organizational Requirements
Section 164.508—Uses and Disclosures for Which Individual Authorization Is Required
Section 164.510—Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object
Section 164.512—Uses and Disclosures for Which Consent, an Authorization, or Opportunity to Agree or Object is Not Required
Section 164.514—Other Procedural Requirements Relating to Uses and

Disclosures of Protected Health Information
Section 164.522—Rights to Request Privacy Protection for Protected Health Information
Section 164.524—Access of Individuals to Protected Health Information
Section 164.526—Amendment of Protected Health Information
Section 164.528—Accounting for Disclosures of Protected Health Information
Section 164.530—Administrative Requirements

C. Comments on Information Collection Requirements in Section A

The Department has submitted a copy of these modifications to the Privacy Rule to OMB for its review and approval of the information collection requirements summarized in Section A above. If you comment on any of the modifications to the information collection and record keeping requirements in §§ 164.506, 164.520, and/or the model business associate contract language 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: Brenda Aguilar, 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 amendments to the Privacy 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 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 amendments with the most direct effect on Federalism principles concerns the clarifications regarding the rights of parents and minors under State law.

The amendments make clear the intent of the Department to defer to State law with respect to such rights. Therefore, the Department believes that the amended Privacy Rule would not significantly affect the rights, roles and responsibilities of States.

X. Sample Business Associate Contract Provisions—Appendix

March 2002 NPRM. In response to requests for guidance, the Department provided sample language for business associate contracts. The provisions were provided as an appendix to the preamble and were intended to serve as guidance for covered entities to assist in compliance with the business associate provisions of the Privacy Rule. The proposal was not a model contract, but rather was sample language that could be included in a contract.

Overview of Public Comment. The Department received a small number of comments addressing the sample business associate contract provisions. The comments fell into four general categories. Most commenters were pleased with the Department's guidance for business associate contracts and expressed appreciation for such guidance. There were some commenters that thought the language was insufficient and requested the Department create a complete model contract not just sample provisions. The third category of commenters thought the provisions went further than the requirements in the regulation and requested specific changes to the sample language. In addition, a few commenters requested that the Department withdraw the sample provisions asserting that they will eliminate the potential of negotiating or establishing a business associate contract that is tailored to the precise requirements of the particular relationship.

Final Modifications. This Rule continues to include sample business associate contract provisions as an appendix to the preamble, because the majority of commenters that addressed this subject found these provisions to be helpful guidance in their compliance efforts with the business associate contract requirements in the Privacy Rule.

The Department has made several changes to the language originally proposed in response to comment. Although these are only sample provisions, the changes, which are described below, should help to clear up some confusion.

First, the Department has changed the name from ''model language'' to ''sample language'' to clarify that the provisions are merely sample clauses, and that none are required to be in a business associate contract so long as the contract meets the requirements of the regulation. The sample language continues to indicate, using square brackets, those instances in which a provision or phrase in a provision applies only in certain circumstances or is optional.

The Department has made three modifications in the Obligations and Activities of the Business Associate provisions. First, there are modifications to clarify that the parties can negotiate appropriate terms regarding the time and manner of providing access to protected health information in a designated record set, providing information to account for disclosures of protected health information, and for making amendments to protected health information in a designated record set. Although the language clarifies that the terms are to be negotiated by the Parties, the agreement must permit the covered entity to comply with its obligations under the Privacy Rule.

Second, the Department has amended the sample language regarding review of business associate practices, books, and records to clarify that the contract must permit the Secretary, not the covered entity, to have access to such records, including protected health information, for purposes of determining the covered entity's compliance with the Privacy Rule. The sample language continues to include the option that parties additionally agree that the business associate shall disclose this information to the covered entity for compliance purposes to indicate that this is still an appropriate approach for this purpose. The modifications also clarify that parties can negotiate the time and manner of providing the covered entity with access to the business associate's internal practices, books, and records.

Finally, the Department has modified the sample language to clarify that business associates are only required to notify the covered entity of uses and disclosures of protected health information not provided for by the agreement of which it becomes aware in order to more closely align the sample contract provisions with the regulation text. The Department did not intend to imply a different standard than that included in the regulation.

The Department has modified the General Use and Disclosure sample language to clarify that there are two possible approaches, and that in each approach the use or disclosure of protected health information by a business associate shall be consistent with the minimum necessary policies and procedures of the covered entity.

The Department has adopted one change to the sample language under Specific Use and Disclosure that clarifies that a permitted specific use of protected health information by the business associate includes reporting violations of law to appropriate Federal and State authorities. This would permit a business associate to use or disclose protected health information in accordance with the standards in § 164.502(j)(1). We indicate that this is optional text, not required by the Privacy Rule. Because we have included this language as sample language, we have deleted discussion of this issue in the statement preceding the sample business associate contract provisions.

Under Obligations of Covered Entity, the Department has clarified that covered entities need only notify business associates of a restriction to the use or disclosure of protected health information in its notice of privacy practices to the extent that such restriction may affect the business associates' use or disclosure of protected health information. The other provisions requiring the covered entity to notify the business associate of restrictions to the use or disclosure of protected health information remain and have been modified to include similar limiting language.

In the Term and Termination provisions, the Department has added clarifying language that indicates that if neither termination nor cure are feasible, the covered entity shall report the violation to the Secretary. We have also clarified that the parties should negotiate how they will determine whether the return or destruction of protected health information is infeasible.

Finally, the Department has clarified the miscellaneous provision regarding interpretation to clarify that ambiguities shall be resolved to permit the covered entity's compliance with the Privacy Rule.

Each entity should carefully analyze each of the sample provisions to ensure that it is appropriate given the specific business associate relationship. Some of the modifications are intended to address some commenters concerns that the sample language is weighted too heavily in favor of the covered entity. Individual parties are reminded that all contract provisions are subject to negotiation, provided that they are consistent with the requirements in the Privacy Rule. The sample language is not intended to, and cannot, substitute for responsible legal advice.

Response to Other Public Comments

Comment: Several commenters noted that the sample language was missing certain required contractual elements, such as an effective date, insurance and indemnification clauses, procedures for amending the contract, as well as other provisions that may be implicated by the Privacy Rule, such as the Electronic Transactions Standards. Some of these commenters requested that the guidance be a complete model contract rather than sample contract provisions so that the covered entity would not need legal assistance.

Response: The Department intentionally did not make this guidance a complete model contract, but rather provided only those provisions specifically tied to requirements of the Privacy Rule. As stated above, this guidance does not substitute for legal advice. Other contract provisions may be dictated by State or other law or by the relationship between the parties. It is not feasible to provide sample contracts that would accommodate each situation. Parties are free to negotiate additional terms, including those that may be required by other laws or regulations.

Comment: Some commenters requested that use of the sample business associate contract language create a safe harbor for an entity that adopts them.

Response: The sample business associate contract provisions are not a safe harbor. Rather, the sample language is intended to provide guidance and assist covered entities in the effort required to enter into a business associate agreement. Use of the sample provisions or similar provisions, where appropriate, would be considered strong evidence of compliance with the business associate contract provisions of the Privacy Rule. However, contracts will necessarily vary based on State law and the relationship between the covered entity and the business associate.

Comment: Some commenters were concerned that the sample provision permitting a covered entity to have access to the practices, books, and records of the business associate would impose an audit requirement on the covered entity.

Response: The sample business associate contract provisions do not impose any additional requirements on covered entities. Only the regulation imposes requirements. Therefore, the inclusion of the provision that the business associate shall allow the covered entity access to the business associate practices, books, and records does not indicate that the Privacy Rule imposes an audit requirement on the covered entity. We have stated numerous times that the Privacy Rule does not require covered entities to monitor the activities of their business associates.

Comment: One commenter noted that the business associate should not be required, under the contract, to mitigate damages resulting from a violation.

Response: We disagree. In order for a covered entity to be able to act as it is required to under the Privacy Rule when a business associate is holding protected health information, the covered entity must require the same activities of the business associate through the contract.

Comment: One commenter noted that the Privacy Rule does not explicitly direct that a covered entity provide its notice of privacy practices to its business associates.

Response: We agree and have modified the language in the sample provision accordingly. However, in order for the business associate to act consistently with the privacy practices of the covered entity, which is required by the Privacy Rule, the parties may find it necessary to require disclosure of these policies. To the extent that parties can craft an alternate approach, they are free to do so.

Comment: One commenter indicated that traditional contract terms such as ''term'' and ''termination'' should not be included in the sample language if the Department's intention is to address only those terms required by the Rule.

Response: Because termination of the business associate agreement is specifically addressed in the Privacy Rule, we have retained these provisions in the sample language. As with all other provisions, parties are free to negotiate alternative Term and Termination provisions that meet their unique situations and concerns,

provided that they meet the requirements of the Privacy Rule.

Comment: Another commenter indicated that the sample language should not require the return or destruction of protected health information in the possession of subcontractors or agents of the business associate.

Response: We have retained this language as this is consistent with the Privacy Rule. Section 164.504(e)(2)(ii)(D) requires that the business associate contract include a provision that the business associate ensures that any agents, including subcontractors, agree to the same restrictions and conditions as the business associate. Generally, the contract must require the business associate to return or destroy protected health information; therefore, the contract also must require the business associate to have agents and subcontractors to do the same. This is reflected in the sample contract language.

Comment: One commenter requested that the sample language include a provision that the covered entity may impose monetary damages on a business associate for violation of its privacy policies.

Response: We have not included such a provision because the Privacy Rule does not address this issue. The Privacy Rule would not prohibit a monetary damages provision from being included in the contract. This, again, is a matter to be negotiated between covered entities and their business associates.

Comment: One commenter suggested that specific references to sections in the Rule be deleted and either replaced by a general statement that the contract shall be interpreted in a manner consistent with the Rule or supplemented with clarifying language with examples.

Response: We believe that using section reference is a valid and expeditious approach as it incorporates changes as modifications are made to the Privacy Rule. A business associate contract may take a different approach than using section references to the Privacy Rule.

Comment: One commenter asked that the sample business associate contract provisions be included in the Rule rather than published as an appendix to the preamble so that it will be in the Code of Federal Regulations.

Response: We have published the sample business associate contract provisions as an appendix to the preamble because they are meant as guidance. The sample language shall be available on the Office for Civil Rights web site at *www.hhs.gov/ocr/hipaa;* and may be updated or revised as necessary.

Appendix to the Preamble—Sample Business Associate Contract Provisions

Statement of Intent

The Department provides these sample business associate contract provisions in response to numerous requests for guidance. This is only sample 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 sample 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. They do not include many formalities and substantive provisions that are required or typically included in a valid contract. Reliance on this sample 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 sample provisions, for example having a business associate create a limited data set. These and other types of issues will need to be worked out between the parties.

Sample Business Associate Contract Provisions [3]

Definitions (Alternative Approaches)

Catch-all definition:

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Privacy Rule.

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 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 to 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 of which it becomes aware.

(e) Business Associate agrees to ensure that any agent, including a

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

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 [Insert negotiated terms], 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 [Insert negotiated terms]. [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, including policies and procedures and Protected Health Information, 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] to the Secretary, in a time and manner [Insert negotiated terms] or designated by 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 [Insert negotiated terms], 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 [(a) and (b) are alternative approaches]

(a) *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 or the minimum necessary policies and procedures of the Covered Entity: [List Purposes].

(b) *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 or the minimum necessary policies and procedures of the Covered Entity.

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).

(d) Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with § 164.502(j)(1).

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 notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.

(b) Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.

(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, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

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. [Term may differ.]

(b) *Termination for Cause.* Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

(1) 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;

(2) 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; or

(3) If neither termination nor cure are feasible, Covered Entity shall report the violation to the Secretary. [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 [Insert negotiated terms] 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.

(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 of 1996, Pub. L. No. 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 to permit 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: August 6, 2002.

Tommy G. Thompson,

Secretary.

For the reasons set forth in the preamble, the Department amends 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. No. 104–191, 110 Stat. 2021–2031 and sec. 264 of Pub. L. No. 104–191 (42 U.S.C. 1320d–2(note)).

2. Amend § 160.102(b), by removing the phrase ''section 201(a)(5) of the Health Insurance Portability Act of 1996, (Pub. L. No. 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.

* * * * *

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. No. 104–191, 110 Stat. 2033–2034 (42 U.S.C. 1320d–2(note)).

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

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

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''.

f. Remove the words ''a covered'' and replace them with ''an'' in the definition of ''required by law''.

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 the 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 or a limited data set, and fundraising for the benefit of the covered entity.

* * * * *

Marketing means:

(1) To make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service, unless the communication is made:

(i) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits.

(ii) For treatment of the individual; or

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

(2) An arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.

* * * * *

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 a new paragraph (g)(3)(ii).

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) 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 use or disclosure;

* * * * *

(vi) As permitted by and in compliance with this section, § 164.512, or § 164.514(e), (f), or (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) If, and to the extent, permitted or required by an applicable provision of State or other law, including applicable case law, a covered entity may disclose, or provide access in accordance with § 164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis*;

(B) If, and to the extent, prohibited by an applicable provision of State or other law, including applicable case law, a covered entity may not disclose, or provide access in accordance with § 164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis*; and

(C) Where the parent, guardian, or other person acting *in loco parentis*, is not the personal representative under paragraphs (g)(3)(i)(A), (B), or (C) of this section and where there is no applicable access provision under State or other law, including case law, a covered entity may provide or deny access under § 164.524 to a parent, guardian, or other person acting *in loco parentis,* if such action is consistent with State or other applicable law, provided that such decision must be made by a licensed health care professional, in the exercise of professional judgment.

* * * * *

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)(2)(ii).

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

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

f. 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

* * * * *

(2) *Implementation specifications: Safeguard requirements.* * * *

(ii) A component that is described by paragraph (c)(3)(iii)(B) of this section does not use or disclose protected health information that it creates or receives from or on behalf of the health care component in a way prohibited by this subpart; 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) also may include a component only to the extent that it performs:

(A) Covered functions; or

(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.

* * * * *

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 for uses and disclosures 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, under paragraph (b) of this section, shall not be effective to permit a use or disclosure of protected health information when an authorization, under § 164.508, is required or when another condition must be met for such use or disclosure to be permissible under 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 a health care provider.

(3) A covered entity may disclose protected health information to another covered entity or a 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 each entity either has or had a relationship with the individual who is the subject of the protected health information being requested, the protected health information pertains to such relationship, 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. Revise § 164.508 to read as follows:

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

(a) *Standard: authorizations for uses and disclosures.*—(1) *Authorization required: general rule.* Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization.

(2) *Authorization required: psychotherapy notes.* Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:

(i) To carry out the following treatment, payment, or health care operations:

(A) Use by the originator of the psychotherapy notes for treatment;

(B) Use or disclosure by the covered entity for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or

(C) Use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual; and

(ii) A use or disclosure that is required by § 164.502(a)(2)(ii) or permitted by § 164.512(a); § 164.512(d) with respect to the oversight of the originator of the psychotherapy notes; § 164.512(g)(1); or § 164.512(j)(1)(i).

(3) *Authorization required: Marketing.* (i) Notwithstanding any provision of this subpart, other than the transition provisions in § 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 involves direct or indirect remuneration to the covered entity from a third party, the authorization must state that such remuneration is involved.

(b) *Implementation specifications: general requirements.*—(1) *Valid authorizations.* (i) A valid authorization is a document that meets the requirements in paragraphs (a)(3)(ii), (c)(1), and (c)(2) of this section, as applicable.

(ii) A valid authorization may contain elements or information in addition to the elements required by this section, provided that such additional elements or information are not inconsistent with the elements required by this section.

(2) *Defective authorizations.* An authorization is not valid, if the document submitted has any of the following defects:

(i) The expiration date has passed or the expiration event is known by the covered entity to have occurred;

(ii) The authorization has not been filled out completely, with respect to an element described by paragraph (c) of this section, if applicable;

(iii) The authorization is known by the covered entity to have been revoked;

(iv) The authorization violates paragraph (b)(3) or (4) of this section, if applicable;

(v) Any material information in the authorization is known by the covered entity to be false.

(3) *Compound authorizations.* An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization, except as follows:

(i) An authorization for the use or disclosure of protected health information for a 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;

(ii) An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes;

(iii) An authorization under this section, other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other such authorization under this section, except when a covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits under paragraph (b)(4) of this section on the provision of one of the authorizations.

(4) *Prohibition on conditioning of authorizations.* A covered entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except:

(i) A covered health care provider may condition the provision of research-related treatment on provision of an authorization for the use or disclosure of protected health information for such research under this section;

(ii) A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan prior to an individual's enrollment in the health plan, if:

(A) The authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations; and

(B) The authorization is not for a use or disclosure of psychotherapy notes under paragraph (a)(2) of this section; and

(iii) A covered entity may condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party on provision of an authorization for the disclosure of the protected health information to such third party.

(5) *Revocation of authorizations.* An individual may revoke an authorization provided under this section at any time, provided that the revocation is in writing, except to the extent that:

(i) The covered entity has taken action in reliance thereon; or

(ii) If the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy or the policy itself.

(6) *Documentation.* A covered entity must document and retain any signed authorization under this section as required by § 164.530(j).

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

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

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

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

(iv) 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 statement ''end of the research study,'' ''none,'' or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including 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 subpart.

(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).

i. In paragraph (i)(2)(iii) remove ''(i)(2)(ii)(D)'' and add in its place ''(i)(2)(ii)(C)''.

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. In paragraph (d)(5), remove the word ''discloses'' and add in its place the word ''disclose''.

e. Revise 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) (1) *Standard: Limited data set.* A covered entity may use or disclose a limited data set that meets the requirements of paragraphs (e)(2) and (e)(3) of this section, if the covered entity enters into a data use agreement with the limited data set recipient, in accordance with paragraph (e)(4) of this section.

(2) *Implementation specification: Limited data set:* A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

(i) Names;

(ii) Postal address information, other than town or city, State, and zip code;

(iii) Telephone numbers;

(iv) Fax numbers;

(v) Electronic mail addresses;
(vi) Social security numbers;
(vii) Medical record numbers;
(viii) Health plan beneficiary numbers;
(ix) Account numbers;
(x) Certificate/license numbers;
(xi) Vehicle identifiers and serial numbers, including license plate numbers;
(xii) Device identifiers and serial numbers;
(xiii) Web Universal Resource Locators (URLs);
(xiv) Internet Protocol (IP) address numbers;
(xv) Biometric identifiers, including finger and voice prints; and
(xvi) Full face photographic images and any comparable images.

(3) *Implementation specification: Permitted purposes for uses and disclosures.* (i) A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only for the purposes of research, public health, or health care operations.

(ii) A covered entity may use protected health information to create a limited data set that meets the requirements of paragraph (e)(2) of this section, or disclose protected health information only to a business associate for such purpose, whether or not the limited data set is to be used by the covered entity.

(4) *Implementation specifications: Data use agreement.*—(i) *Agreement required.* A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only if the covered entity obtains satisfactory assurance, in the form of a data use agreement that meets the requirements of this section, that the limited data set recipient will only use or disclose the protected health information for limited purposes.

(ii) *Contents.* A data use agreement between the covered entity and the limited data set recipient must:

(A) Establish the permitted uses and disclosures of such information by the limited data set recipient, consistent with paragraph (e)(3) of this section. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity;

(B) Establish who is permitted to use or receive the limited data set; and

(C) Provide that the limited data set recipient will:

(*1*) Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;

(*2*) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;

(*3*) Report to the covered entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;

(*4*) Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and

(*5*) Not identify the information or contact the individuals.

(iii) *Compliance.* (A) A covered entity is not in compliance with the standards in paragraph (e) of this section if the covered entity knew of a pattern of activity or practice of the limited data set recipient that constituted a material breach or violation of the data use agreement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:

(1) Discontinued disclosure of protected health information to the recipient; and

(2) Reported the problem to the Secretary.

(B) A covered entity that is a limited data set recipient and violates a data use agreement will be in noncompliance with the standards, implementation specifications, and requirements of paragraph (e) of this section.

* * * * *

12. Amend § 164.520 as follows:

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

b. In paragraph (c), introductory text, remove ''(c)(4)'' and add in its place ''(c)(3)''.

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

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

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

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

g. Amend paragraph (c)(3)(iii) by adding a sentence at the end.

h. 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.

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. Remove the word ''or'' from paragraph (a)(1)(v).

c. Redesignate paragraph (a)(1)(vi) as (a)(1)(ix) and redesignate paragraphs (a)(1)(iii) through (v) as (a)(1)(v) through (vii).

d. Add paragraphs (a)(1)(iii), (iv), and (a)(1)(viii).

e. Revise paragraph (b)(2), introductory text.

f. Revise paragraph (b)(2)(iv).

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

h. Add paragraph (b)(4).

The additions and revisions 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) Incident to a use or disclosure otherwise permitted or required by this subpart, as provided in § 164.502;

(iv) Pursuant to an authorization as provided in § 164.508;

* * * * *

(viii) As part of a limited data set in accordance with § 164.514(e); or

* * * * *

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

(2) Except as otherwise provided by paragraphs (b)(3) or (b)(4) of this section, the accounting must include for each disclosure:

* * * * *

(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.

* * * * *

(4)(i) If, during the period covered by the accounting, the covered entity has made disclosures of protected health information for a particular research purpose in accordance with § 164.512(i) for 50 or more individuals, the accounting may, with respect to such disclosures for which the protected health information about the individual may have been included, provide:

(A) The name of the protocol or other research activity;

(B) A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;

(C) A brief description of the type of protected health information that was disclosed;

(D) The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;

(E) The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and

(F) A statement that the protected health information of the individual may or may not have been disclosed for a particular protocol or other research activity.

(ii) If the covered entity provides an accounting for research disclosures, in accordance with paragraph (b)(4) of this section, and if it is reasonably likely that the protected health information of the individual was disclosed for such research protocol or activity, the covered entity shall, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.

* * * * *

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, to the extent allowed by one of the following permissions, use or disclose, for research, 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 the covered entity has obtained, prior to the applicable compliance date, either:

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

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

(3) A waiver, by an IRB, of informed consent for the research, 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.

(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 October 15, 2002, 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

October 15, 2002, 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, 164.528, and 164.530(f) with respect to protected health information held by a business associate.

[FR Doc. 02–20554 Filed 8–9–02; 2:00 pm]

BILLING CODE 4153–01–P