Federal Register

Wednesday,
July 14, 2010

Part II

Department of Health and Human Services

45 CFR Parts 160 and 164

Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act; Proposed Rule

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Parts 160 and 164

RIN: 0991–AB57

Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act

AGENCY: Office for Civil Rights, Department of Health and Human Services.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Department of Health and Human Services (HHS or "the Department") is issuing this notice of proposed rulemaking to modify the Standards for Privacy of Individually Identifiable Health Information (Privacy Rule), the Security Standards for the Protection of Electronic Protected Health Information (Security Rule), and the rules pertaining to Compliance and Investigations, Imposition of Civil Money Penalties, and Procedures for Hearings (Enforcement Rule) issued under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The purpose of these modifications is to implement recent statutory amendments under the Health Information Technology for Economic and Clinical Health Act ("the HITECH Act" or "the Act"), to strengthen the privacy and security protection of health information, and to improve the workability and effectiveness of these HIPAA Rules.

DATES: Submit comments on or before September 13, 2010.

ADDRESSES: You may submit comments, identified by RIN 0991–AB57, by any of the following methods (please do not submit duplicate comments):

• *Federal eRulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments. Attachments should be in Microsoft Word, WordPerfect, or Excel; however, we prefer Microsoft Word.

• *Regular, Express, or Overnight Mail:* U.S. Department of Health and Human Services, Office for Civil Rights, Attention: HITECH Privacy and Security Rule Modifications, Hubert H. Humphrey Building, Room 509F, 200 Independence Avenue, SW., Washington, DC 20201. Please submit one original and two copies.

• *Hand Delivery or Courier:* Office for Civil Rights, Attention: HITECH Privacy and Security Rule Modifications, Hubert H. Humphrey Building, Room 509F, 200 Independence Avenue, SW., Washington, DC 20201. Please submit one original and two copies. (Because access to the interior of the Hubert H. Humphrey Building is not readily available to persons without Federal government identification, commenters are encouraged to leave their comments in the mail drop slots located in the main lobby of the building.)

Inspection of Public Comments: All comments received before the close of the comment period will be available for public inspection, including any personally identifiable or confidential business information that is included in a comment. We will post all comments received before the close of the comment period at *http://www.regulations.gov.* Because comments will be made public, they should not include any sensitive personal information, such as a person's social security number; date of birth; driver's license number, State identification number or foreign country equivalent; passport number; financial account number; or credit or debit card number. Comments also should not include any sensitive health information, such as medical records or other individually identifiable health information, or any non-public corporate or trade association information, such as trade secrets or other proprietary information.

FOR FURTHER INFORMATION CONTACT: Andra Wicks, 202–205–2292.

SUPPLEMENTARY INFORMATION:

The discussion below includes a description of the statutory and regulatory background of the proposed rules, a section-by-section description of the proposed modifications, and the impact statement and other required regulatory analyses. We solicit public comment on the proposed rules. Persons interested in commenting on the provisions of the proposed rules can assist us by preceding discussion of any particular provision or topic with a citation to the section of the proposed rule being discussed.

I. Statutory and Regulatory Background

The regulatory modifications proposed below concern several sets of rules that implement the Administrative Simplification provisions of title II, subtitle F, of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub. L. 104–191), which added a new part C to title XI of the Social Security Act (sections 1171–1179 of the Social Security Act, 42 U.S.C. 1320d–1320d–8). The Health Information Technology for Economic and Clinical Health (HITECH) Act, which was enacted as title XIII of division A and title IV of division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Public Law 111–5, modifies certain provisions of the Social Security Act pertaining to the Administrative Simplification Rules (HIPAA Rules) and requires certain modifications to the HIPAA Rules themselves.

A. HIPAA Administrative Simplification—Statutory Background

The Administrative Simplification provisions of HIPAA provided for the establishment of national standards for the electronic transmission of certain health information, such as standards for certain health care transactions conducted electronically and code sets and unique health care identifiers for health care providers and employers. The Administrative Simplification provisions of HIPAA also required the establishment of national standards to protect the privacy and security of personal health information and established civil money and criminal penalties for violations of the Administrative Simplification provisions. The Administrative Simplification provisions of HIPAA apply to three types of entities, which are known as "covered entities": health care providers who conduct covered health care transactions electronically, health plans, and health care clearinghouses.

B. HIPAA Administrative Simplification—Regulatory Background

The rules proposed below concern the privacy and security standards issued pursuant to HIPAA, as well as the enforcement rules that implement HIPAA's civil money penalty authority. The Standards for Privacy of Individually Identifiable Health Information, known as the "Privacy Rule," were issued on December 28, 2000, and amended on August 14, 2002. *See* 65 FR 82462, as amended at 67 FR 53182. The Security Standards for the Protection of Electronic Protected Health Information, known as the "Security Rule," were issued on February 20, 2003. *See* 68 FR 8334. The Compliance and Investigations, Imposition of Civil Money Penalties, and Procedures for Hearings regulations, collectively known as the "Enforcement Rule," were issued as an interim final rule on April 17, 2003 (68 FR 18895), and revised and issued as a final rule, following rulemaking, on February 16, 2006 (71 FR 8390).

The Privacy Rule protects individuals' medical records and other individually

identifiable health information created or received by or on behalf of covered entities, known as "protected health information." The Privacy Rule protects individuals' health information by regulating the circumstances under which covered entities may use and disclose protected health information and by requiring covered entities to have safeguards in place to protect the privacy of the information. As part of these protections, covered entities are required to have contracts or other arrangements in place with business associates that perform functions for or provide services to the covered entity and that require access to protected health information to ensure that these business associates likewise protect the privacy of the health information. The Privacy Rule also gives individuals rights with respect to their protected health information, including rights to examine and obtain a copy of their health records and to request corrections.

The Security Rule, which applies only to protected health information in electronic form, requires covered entities to implement certain administrative, physical, and technical safeguards to protect this electronic information. As with the Privacy Rule, the Security Rule requires covered entities to have contracts or other arrangements in place with their business associates that provide satisfactory assurances that the business associates will appropriately safeguard the electronic protected health information they receive, create, maintain, or transmit on behalf of the covered entities.

The Enforcement Rule establishes rules governing the compliance responsibilities of covered entities with respect to cooperation in the enforcement process. It also provides rules governing the investigation by the Department of compliance by covered entities, both through the investigation of complaints and the conduct of compliance reviews. It establishes rules governing the process and grounds for establishing the amount of a civil money penalty where the Department has determined a covered entity has violated a requirement of a HIPAA Rule. Finally, the Enforcement Rule establishes rules governing the procedures for hearings and appeals where the covered entity challenges a violation determination.

C. The HITECH Act—Statutory Background

The HITECH Act, enacted on February 17, 2009, is designed to promote the widespread adoption and standardization of health information technology. Subtitle D of title XIII, entitled "Privacy," supports this goal by adopting amendments designed to strengthen the privacy and security protections of health information established by HIPAA. These provisions include extending the applicability of certain of the Privacy and Security Rules' requirements to the business associates of covered entities; requiring HIPAA covered entities and business associates to provide for notification of breaches of "unsecured protected health information"; establishing new limitations on the use and disclosure of protected health information for marketing and fundraising purposes; prohibiting the sale of protected health information; requiring the consideration of a limited data set as the minimum necessary amount of information; and expanding individuals' rights to access and receive an accounting of disclosures of their protected health information, and to obtain restrictions on certain disclosures of protected health information to health plans. In addition, subtitle D adopts provisions designed to strengthen and expand HIPAA's enforcement provisions. We provide a brief overview of the relevant statutory provisions below.

In the area of business associates, the Act makes a number of changes. First, section 13401 of the Act applies certain provisions of the Security Rule that apply to covered entities directly to their business associates and makes business associates liable for civil and criminal penalties for the failure to comply with these provisions. Similarly, section 13404 makes business associates of covered entities civilly and criminally liable under the Privacy Rule for making uses and disclosures of protected health information that do not comply with the terms of their business associate contracts. The Act also provides that the additional privacy and security requirements of subtitle D of the Act are applicable to business associates and that such requirements shall be incorporated into business associate contracts. Finally, section 13408 of the Act requires that organizations that provide data transmission of protected health information to a covered entity or business associate and that require routine access to such information, such as Health Information Exchange Organizations, Regional Health Information Organizations, and E-prescribing Gateways, as well as vendors that contract with covered entities to offer personal health records to patients as part of the covered entities' electronic health records, shall be treated as business associates for purposes of the HITECH Act and the HIPAA Privacy and Security Rules and required to enter into business associate contracts.

Section 13402 of the Act sets forth the breach notification provisions, requiring covered entities and business associates to provide notification following discovery of a breach of unsecured protected health information. Additionally, section 13407 of the Act, enforced by the Federal Trade Commission (FTC), applies similar breach notification provisions to vendors of personal health records and their third party service providers.

Section 13405 of the Act requires the Department to modify certain Privacy Rule provisions. In particular, section 13405 sets forth certain circumstances in which covered entities must comply with an individual's request for restriction of disclosure of his or her protected health information, provides for covered entities to consider a limited data set as the minimum necessary for a particular use, disclosure, or request of protected health information, and requires the Secretary to issue guidance to address what constitutes minimum necessary under the Privacy Rule. Section 13405 also requires the Department to modify the Privacy Rule to require covered entities that use or maintain electronic health records to provide individuals, upon request, with an accounting of disclosures of protected health information through an electronic health record for treatment, payment, or health care operations; generally prohibits the sale of protected health information without a valid authorization from the individual; and strengthens an individual's right to an electronic copy of their protected health information, where a covered entity uses or maintains an electronic health record.

Section 13406 of the Act requires the Department to modify the marketing and fundraising provisions of the Privacy Rule. With respect to marketing, the Act requires authorizations for certain health-related communications, which are currently exempted from the definition of marketing, if the covered entity receives remuneration in exchange for making the communication. The Act also strengthens an individual's right under the Privacy Rule to opt out of fundraising communications by requiring the Department to modify the Privacy Rule so that covered entities must provide individuals with a clear and conspicuous opportunity to opt out of receiving fundraising

communications and by requiring that an opt out be treated as a revocation of authorization under the Privacy Rule.

Section 13410 of the Act addresses enforcement in a number of ways. First, section 13410(a) provides that the Secretary's authority to impose a civil money penalty will only be barred to the extent a criminal penalty has been *imposed*, rather than in cases in which the offense in question merely constitutes an offense criminally *punishable.* In addition, section 13410(a) of the Act requires the Secretary to formally investigate any complaint where a preliminary investigation of the facts indicates a possible violation due to willful neglect and to impose a penalty where a violation is found in such cases. Section 13410(c) of the Act provides, for purposes of enforcement, for the transfer to the HHS Office for Civil Rights of any civil money penalty or monetary settlement collected under the Privacy and Security Rules and also requires the Department to establish by regulation a methodology for distributing to harmed individuals a percentage of the civil money penalties and monetary settlements collected under the Privacy and Security Rules. Effective as of February 18, 2009, section 13410(d) of the Act also modified the civil money penalty structure for violations of the HIPAA Rules by implementing a tiered increase in the amount of penalties based on culpability. In addition, as of February 18, 2009, section 13410(e) of the Act also granted State Attorneys General the authority to enforce the HIPAA Rules by bringing civil actions on behalf of State residents in court.

Section 13421 states that HIPAA's State preemption provisions at 42 U.S.C. 1320d–7 shall apply to the provisions of subtitle D of the HITECH Act in the same manner as they do to HIPAA's provisions.[1] Section 13423 of the Act provides a general effective date of February 18, 2010, for most of its provisions, except where a different effective date is otherwise provided.

The Act also provides for the development of guidance, reports, and studies in a number of areas, including guidance on appropriate technical safeguards to implement the HIPAA Security Rule (section 13401(c)); for purposes of breach notification, guidance on the methods and technologies for rendering protected health information unusable, unreadable, or indecipherable to unauthorized individuals (section 13402(h)); guidance on what constitutes the minimum necessary amount of information for purposes of the Privacy Rule (section 13405(b)); a report by the Government Accountability Office (GAO) regarding recommendations for a methodology under which harmed individuals may receive a percentage of civil money penalties and monetary settlements under the HIPAA Privacy and Security Rules (section 13410(c)); a report to Congress on HIPAA Privacy and Security enforcement (section 13424(a)); a study and report on the application of privacy and security requirements to non-HIPAA covered entities (section 13424(b)); guidance on de-identification (section 13424(c)); and a study on the Privacy Rule's definition of "psychotherapy notes" at 45 CFR 164.501, with regard to including test data that is related to direct responses, scores, items, forms, protocols, manuals, or other materials that are part of a mental health evaluation (section 13424(f)).

Finally, the Act includes provisions for education by HHS on health information privacy and for periodic audits by the Secretary. Section 13403(a) provides for the Secretary to designate HHS regional office privacy advisors to offer guidance and education to covered entities, business associates, and individuals on their rights and responsibilities related to Federal privacy and security requirements for protected health information. Section 13403(b) requires the HHS Office for Civil Rights, not later than 12 months after enactment, to develop and maintain a multi-faceted national education initiative to enhance public transparency regarding the uses of protected health information, including programs to educate individuals about potential uses of their protected health information, the effects of such uses, and the rights of individuals with respect to such uses. Section 13411 requires the Secretary to provide for periodic audits to ensure covered entities and business associates comply with the applicable requirements of the HIPAA Privacy and Security Rules.

We discuss many of the Act's statutory provisions in more detail below where we describe section-by-section how these proposed regulations would implement those provisions of the Act. However, we do not discuss in detail the breach notification provisions in sections 13402 of the Act or the modified civil money penalty structure in section 13410(d) of the Act, which as explained below, have been the subject of previous rulemakings. In addition, we do not address in this rulemaking the accounting for disclosures requirement in section 13405 of the Act, which is tied to the adoption of a standard under the HITECH Act at subtitle A of title XIII of ARRA, or the penalty distribution methodology requirement in section 13410(c) of the Act, which is to be based on the recommendations noted above to be developed at a later date by the GAO. These provisions will be the subject of future rulemakings. Further, we clarify that we are not issuing regulations with respect to the new authority of the State Attorneys General to enforce the HIPAA Rules. Finally, other than the guidance required by section 13405(b) of the Act with respect to what constitutes minimum necessary, this proposed rule does not address the studies, reports, guidance, audits, or education efforts required by the HITECH Act.

D. The HITECH Act—Regulatory Background

As noted above, certain of the HITECH Act's privacy and security provisions have already been the subject of rulemakings and related actions. In particular, the Department published interim final regulations to implement the breach notification provisions at section 13402 of the Act for HIPAA covered entities and business associates in the **Federal Register** on August 24, 2009 (74 FR 42740), effective September 23, 2009. Similarly, the FTC published final regulations implementing the breach notification provisions at section 13407 for personal health record vendors and their third party service providers on August 25, 2009 (74 FR 42962), effective September 24, 2009. For purposes of determining to what information the HHS and FTC breach notification regulations apply, the Department also issued, first on April 17, 2009 (published in the **Federal Register** on April 27, 2009, 74 FR 19006), and then later with its interim final rule, the guidance required by the HITECH Act under 13402(h) specifying the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals. In addition, to conform the provisions of the Enforcement Rule to the new tiered and increased civil money penalty structure made effective by the HITECH Act on the day after enactment, or February 18, 2009, the Department published an interim final rule on October 30, 2009 (74 FR 56123), effective November 30, 2009.

[1] We note that section 13421 of the HITECH Act and HIPAA's State preemption provisions do not affect the applicability of other Federal law, such as the Confidentiality of Alcohol and Drug Abuse Patient Records Regulation at 42 CFR Part 2, to a covered entity's use or disclosure of health information.

II. General Issues

A. Effective and Compliance Dates

As noted above, section 13423 of the Act provides that the provisions in subtitle D took effect one year after enactment, *i.e.,* on February 18, 2010, except as specified otherwise. There are a number of exceptions to this general rule. Some provisions were effective the day after enactment, *i.e.,* February 18, 2009. For example, the tiered and increased civil money penalty provisions of section 13410(d) were effective for violations occurring after the date of enactment. Sections 13402 and 13407 of the Act regarding breach notification required interim final rules within 180 days of enactment, with effective dates 30 days after the publication of such rules. Other provisions of the Act have later effective dates. For example, the provision at section 13410(a)(1) of the Act providing that the Secretary's authority to impose a civil money penalty will only be barred to the extent a criminal penalty has been *imposed,* rather than in cases in which the offense in question merely constitutes an offense that is criminally *punishable,* becomes effective for violations occurring on or after February 18, 2011. The rules proposed below generally pertain to the statutory provisions that became effective on February 18, 2010, or, in a few cases, on a later date.

We note that the final rule will not take effect until after most of the provisions of the HITECH Act became effective on February 18, 2010. We recognize that it will be difficult for covered entities and business associates to comply with the statutory provisions until after we have finalized our changes to the HIPAA Rules. In addition, we recognize that covered entities and business associates will need some time beyond the effective date of the final rule to come into compliance with the final rule's provisions. In light of these considerations, we intend to provide covered entities and business associates with 180 days beyond the effective date of the final rule to come into compliance with most of the rule's provisions. We believe that providing a 180-day compliance period best comports with section 1175(b)(2) of the Social Security Act, 42 U.S.C. 1320d–4, and our implementing provision at 45 CFR 160.104(c)(1), which require the Secretary to provide at least a 180-day period for covered entities to comply with modifications to standards and implementation specifications in the HIPAA Rules. While the Social Security Act and the HIPAA Rules permit the Secretary to further delay the compliance date for small health plans, we do not believe that it is necessary to do so for this rule both because most of the changes being proposed are discrete modifications to existing requirements of the HIPAA Rules, as well as because the Department is proposing an additional one-year transition period to modify certain business associate agreements, which should provide sufficient relief to all covered entities, including small health plans. The Department welcomes comment on the assumption that it is not necessary to extend the compliance date for small health plans.

We also expect that for future modifications to the HIPAA Rules, in most cases, a 180-day compliance period will suffice. Accordingly, we propose to add a provision at § 160.105 to address the compliance date generally for implementation of new or modified standards in the HIPAA Rules. Proposed § 160.105 would provide that with respect to new standards or implementation specifications or modifications to standards or implementation specifications in the HIPAA Rules, except as otherwise provided, covered entities and business associates must comply with the applicable new standards or implementation specifications or modifications to standards or implementation specifications no later than 180 days from the effective date of any such change. Where future modifications to the HIPAA Rules necessitate a longer compliance period, we would provide so accordingly in the regulatory text. We propose to retain the compliance date provisions at §§ 164.534 and 164.318, which provide the compliance dates of April 14, 2003, and April 20, 2005, for initial implementation of the HIPAA Privacy and Security Rules, respectively, for historical purposes only.

We note that proposed § 160.105 regarding the compliance date of new or modified standards or implementation specifications would not apply to modifications to the provisions of the HIPAA Enforcement Rule because such provisions are not standards or implementation specifications (as the terms are defined at § 160.103). Such provisions are in effect and apply at the time the final rule becomes effective or as otherwise specifically provided. We also note that our proposed general rule for a 180-day compliance period for new or modified standards would not apply where we expressly provide a different compliance period in the regulation for one or more provisions. For purposes of this proposed rule, this would mean that the 180-day compliance period would not govern the time period required to modify those business associate agreements that qualify for the longer transition period proposed in § 164.532. We seek comments on any potential unintended consequences of establishing a 180-day compliance date as a regulatory default, with the noted exceptions.

B. Other Proposed Changes

While passage of the HITECH Act necessitates much of the rulemaking below, it does not account for all of the proposed changes to the HIPAA Privacy, Security, and Enforcement Rules encompassed in this rulemaking. The Department is taking this opportunity to improve the workability and effectiveness of all three sets of HIPAA Rules. The Privacy Rule has not been amended since 2002, and the Security Rule has not been amended since 2003. While the Enforcement Rule was amended in the October 30, 2009, interim final rule to incorporate the enforcement-related HITECH statutory changes that are already effective, it has not been otherwise substantively amended since 2006. In the intervening years, HHS has accumulated a wealth of experience with these rules, both from public contact in various forums and through the process of enforcing the rules. In addition, we have identified a number of needed technical corrections to the rules. Accordingly, we propose a number of modifications that we believe will eliminate ambiguities in the rules and/or make them more workable and effective. Further, we propose a few modifications to conform the HIPAA Privacy Rule to provisions in the Patient Safety and Quality Improvement Act of 2005 (PSQIA). We address the substantive proposed changes in the section-by-section description of the proposed rule below. Technical corrections are discussed at the end of the section-by-section description of the other proposed amendments to the rules.

III. Section-by-Section Description of the Proposed Amendments to Subparts A and B of Part 160

Subpart A of part 160 of the HIPAA Rules contains general provisions that apply to all of the HIPAA Rules. Subpart B of part 160 contains the regulatory provisions implementing HIPAA's preemption provisions. We propose to amend a number of these provisions. Some of the proposed changes are necessitated by the statutory changes made by the HITECH Act, while others are of a technical or conforming nature.

A. Subpart A—General Provisions, Section 160.101—Statutory Basis and Purpose

This section sets out the statutory basis and purpose of the HIPAA Rules. We propose a technical change to include a reference to the provisions of the HITECH Act upon which most of the regulatory changes proposed below are based.

B. Subpart A—General Provisions, Section 160.102—Applicability

This section sets out to whom the HIPAA Rules apply. We propose to add a new paragraph (b) to make clear, consistent with the provisions of the HITECH Act that are discussed more fully below, that the standards, requirements, and implementation specifications of the subchapter apply to business associates, where so provided.

C. Subpart A—General Provisions, Section 160.103—Definitions

Section 160.103 contains definitions of terms that appear throughout the HIPAA Rules. For ease of reference, we propose to move several definitions currently found at § 160.302 to § 160.103 without substantive change to the definitions themselves. This category includes definitions of the following terms: "ALJ," "civil money penalty," and "violation or violate." As the removal of these definitions, along with the removal of other definitions discussed below (*e.g.,* "administrative simplification provision" and "respondent"), would leave § 160.302 unpopulated, we propose to reserve that section. We also propose to remove a comma from the definition of "disclosure" inadvertently inserted into the definition in a prior rulemaking, which is not intended as a substantive change to the definition. In addition, we propose to replace the term "individually identifiable health information" with "protected health information" in the definition of "standard" to better reflect the scope of the Privacy and Security Rules. Further, we propose the following definitional changes:

1. Definition of "Administrative Simplification Provision"

This definition is currently located in the definitions section of subpart C of part 160 of the HIPAA Enforcement Rule. We propose to remove the definition of this term from § 160.302 and move it to the definitions section located at § 160.103 for clarity and convenience, as the term is used repeatedly throughout the entire part 160. We also propose to add to the definition a reference to sections 13400–13424 of the HITECH Act.

2. Definition of "Business Associate"

Sections 164.308(b) of the Security Rule and 164.502(e) of the Privacy Rule require a covered entity to enter into a contract or other written agreement or arrangement with its business associates. The purpose of these contracts or other arrangements, generally known as business associate agreements, is to provide some legal protection when protected health information is being handled by another person (a natural person or legal entity) on behalf of a covered entity. The HIPAA Rules define "business associate" generally to mean a person who performs functions or activities on behalf of, or certain services for, a covered entity that involve the use or disclosure of protected health information. Examples of business associates include third party administrators or pharmacy benefit managers for health plans, claims processing or billing companies, transcription companies, and persons who perform legal, actuarial, accounting, management, or administrative services for covered entities and who require access to protected health information. We propose a number of modifications to the definition of "business associate." In particular, we propose to modify the definition to conform the term to the statutory provisions of PSQIA, 42 U.S.C. 299b–21, *et seq.,* and the HITECH Act. Additional modifications are made for the purpose of clarifying circumstances when a business associate relationship exists and for general clarification of the definition.

a. Inclusion of Patient Safety Organizations

We propose to add patient safety activities to the list of functions and activities a person may undertake on behalf of a covered entity that give rise to a business associate relationship. PSQIA, at 42 U.S.C. 299b–22(i)(1), provides that Patient Safety Organizations (PSOs) must be treated as business associates when applying the Privacy Rule. PSQIA provides for the establishment of PSOs to receive reports of patient safety events or concerns from providers and provide analyses of events to reporting providers. A reporting provider may be a HIPAA covered entity and, thus, information reported to a PSO may include protected health information that the PSO may analyze on behalf of the covered provider. The analysis of such information is a patient safety activity for purposes of PSQIA and the Patient Safety Rule, 42 CFR 3.10, *et seq.* While the HIPAA Rules as written would encompass a PSO as a business associate when the PSO was performing quality analyses and other activities on behalf of a covered health care provider, we propose this change to the definition of business associate to more clearly align the HIPAA and Patient Safety Rules.

We note that in some cases a covered health care provider, such as a public or private hospital, may have a component PSO that performs patient safety activities on behalf of the health care provider. *See* 42 CFR 3.20. In such cases, the component PSO would not be a business associate of the covered entity but rather the persons performing patient safety activities would be workforce members of the covered entity. However, if the component PSO contracts out some of its patient safety activities to a third party, the third party would be a business associate of the covered entity. In addition, if a component PSO of one covered entity performs patient safety activities for another covered entity, such component PSO would be a business associate of the other covered entity.

b. Inclusion of Health Information Organizations (HIO), E–Prescribing Gateways, and Other Persons That Facilitate Data Transmission; as Well as Vendors of Personal Health Records

Section 13408 of the HITECH Act, which became effective on February 18, 2010, provides that an organization, such as a Health Information Exchange Organization, E-prescribing Gateway, or Regional Health Information Organization, that provides data transmission of protected health information to a covered entity (or its business associate) and that requires access on a routine basis to such protected health information must be treated as a business associate for purposes of the Act and the HIPAA Privacy and Security Rules. Section 13408 also provides that a vendor that contracts with a covered entity to allow the covered entity to offer a personal health record to patients as part of the covered entity's electronic health record shall be treated as a business associate. Section 13408 requires that such organizations and vendors enter into a written business associate contract or other arrangement with the covered entity in accordance with the HIPAA Rules.

In accordance with the Act, we propose to modify the definition of "business associate" to explicitly designate these persons as business

associates. Under proposed paragraphs (3)(i) and (ii) of the definition, the term "business associate" would include: (1) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires routine access to such protected health information; and (2) a person who offers a personal health record to one or more individuals on behalf of a covered entity.

Section 13408 of the Act makes reference to Health Information Exchange Organizations; however, we instead include in the proposed definition the term "Health Information Organization" because it is our understanding that "Health Information Organization" is the more widely recognized and accepted term to describe an organization that oversees and governs the exchange of health-related information among organizations.[2] Section 13408 of the Act also specifically refers to Regional Health Information Organizations. However, we do not believe the inclusion of the term in the definition of "business associate" is necessary as a Regional Health Information Organization is simply a Health Information Organization that governs health information exchange among organizations within a defined geographic area.[3] Further, the specific terms of "Health Information Organization" and "E-prescribing Gateway" are merely illustrative of the types of organizations that would fall within this paragraph of the definition of "business associate." We request comment on the use of these terms within the definition and whether additional clarifications or additions are necessary.

Section 13408 also provides that the data transmission organizations that the Act requires to be treated as business associates are those that require access to protected health information on a routine basis. Conversely, data transmission organizations that do not require access to protected health information on a routine basis would not be treated as business associates. This is consistent with our prior interpretation of the definition of "business associate," through which we have indicated that entities that act as mere conduits for the transport of protected health information but do not access the information other than on a random or infrequent basis are not business associates. *See http://www.hhs.gov/ocr/privacy/hipaa/faq/providers/business/245.html.* In contrast, however, entities that manage the exchange of protected health information through a network, including providing patient locator services and performing various oversight and governance functions for electronic health information exchange, have more than "random" access to protected health information and thus, would fall within the definition of "business associate."

c. Inclusion of Subcontractors

We propose to add language in paragraph (3)(iii) of the definition of "business associate" to provide that subcontractors of a covered entity—*i.e.,* those persons that perform functions for or provide services to a business associate, other than in the capacity as a member of the business associate's workforce, are also business associates to the extent that they require access to protected health information. We also propose to include a definition of "subcontractor" in § 160.103 to make clear that a subcontractor is a person who acts on behalf of a business associate, other than in the capacity of a member of the workforce of such business associate. Even though we use the term "subcontractor," which implies there is a contract in place between the parties, we note that the definition would apply to an agent or other person who acts on behalf of the business associate, even if the business associate has failed to enter into a business associate contract with the person. We request comment on the use of the term "subcontractor" and its proposed definition.

The proposed modifications are similar in structure and effect to the Privacy Rule's initial extension of privacy protections from covered entities to business associates through contract requirements to protect downstream protected health information. The proposed provisions avoid having privacy and security protections for protected health information lapse merely because a function is performed by an entity that is a subcontractor rather than an entity with a direct relationship with a covered entity. Allowing such a lapse in privacy and security protections may allow business associates to avoid liability imposed upon them by sections 13401 and 13404 of the Act, thus circumventing the congressional intent underlying these provisions. The proposed definition of "subcontractor" also is consistent with Congress' overall concern that the privacy and security protections of the HIPAA Rules extend beyond covered entities to those entities that create or receive protected health information in order for the covered entity to perform its health care functions. For example, as discussed above, section 13408 makes explicit that certain types of entities providing services to covered entities—*e.g.,* vendors of personal health records—shall be considered business associates. Therefore, consistent with Congress' intent in sections 13401 and 13404 of the Act, as well as its overall concern that the HIPAA Rules extent beyond covered entities to those entities that create or receive protected health information, we propose that downstream entities that work at the direction of or on behalf of a business associate and handle protected health information would also be required to comply with the applicable Privacy and Security Rule provisions in the same manner as the primary business associate, and likewise would incur liability for acts of noncompliance. We note, and further explain below, that this proposed modification would not require the covered entity to have a contract with the subcontractor; rather, the obligation would remain on each business associate to obtain satisfactory assurances in the form of a written contract or other arrangement that a subcontractor will appropriately safeguard protected health information. For example, under this proposal, if a business associate, such as a third party administrator, hires a company to handle document and media shredding to securely dispose of paper and electronic protected health information, then the shredding company would be directly required to comply with the applicable requirements of the HIPAA Security Rule (*e.g.,* with respect to proper disposal of electronic media) and the Privacy Rule (*e.g.,* with respect to limiting its uses and disclosures of the protected health information in accordance with its contract with the business associate).

d. Exceptions to Business Associate

We also propose to move the provisions at §§ 164.308(b)(2) and 164.502(e)(1)(ii) to the definition of business associate. These provisions provide that in certain circumstances, such as when a covered entity discloses protected health information to a health care provider concerning the treatment of an individual, a covered entity is not required to enter into a business

[2] Department of Health and Human Services, Office of the National Coordinator for Health Information Technology, The National Alliance for Health Information Technology Report to the Office of the National Coordinator For Health Information Technology: Defining Key Health Information Terms, Pg. 24 (2008).

[3] *Id.* at 25.

associate contract or other arrangement with the recipient of the protected health information. While we do not change the meaning of these provisions, we believe these limitations on the scope of "business associate" are more appropriately placed in the definition as exceptions to the term to make clear that the Department does not consider the recipients of the protected health information in these circumstances to be business associates. The movement of these exceptions and refinement of the definition of "business associate" also would help clarify that a person is a business associate if it meets the definition of "business associate," even if a covered entity, or business associate with respect to a subcontractor, fails to enter into the required contract with the business associate.

e. Technical Changes to the Definition

For clarity and consistency, we also propose to change the term "individually identifiable health information" in the current definition of "business associate" to "protected health information," since a business associate has no obligations under the HIPAA Rules with respect to individually identifiable health information that is not protected health information.

3. Definition of "Compliance Date"

The term "compliance date" currently refers only to covered entities. We propose a technical change to include business associates in the term, in light of the HITECH Act amendments, which apply certain provisions of the HIPAA Rules to business associates.

4. Definition of "Electronic Media"

The term "electronic media" was originally defined in the Transactions and Code Sets Rule issued on August 17, 2000 (65 FR 50312) and was included in the definitions at § 162.103. That definition was subsequently revised and moved to § 160.103. The purpose of the revision was to clarify that—

> the physical movement of electronic media from place to place is not limited to magnetic tape, disk, or compact disk. This clarification removes a restriction as to what is considered to be physical electronic media, thereby allowing for future technological innovation. We further clarified that transmission of information not in electronic form before the transmission, for example, paper or voice, is not covered by this definition.

68 FR 8339, Feb. 20, 2003.

We propose to revise the definition of "electronic media" in the following ways. First, we would revise paragraph (1) of the definition to conform it to current usage, as set forth in "Guidelines for Media Sanitization" (*Definition of Medium,* NIST SP 800–88, Glossary B, p. 27 (2006)). The NIST definition, which was updated subsequent to the issuance of the Privacy and Security Rules, was developed in recognition of the likelihood that the evolution of development of new technology would make use of the term "electronic storage media" obsolete in that there may be "storage material" other than "media" that house electronic data. Second, we would add to paragraph (2) of the definition of "electronic media" a reference to intranets, to clarify that intranets come within the definition. Third, we propose to change the word "because" to "if" in the final sentence of paragraph (2) of the definition of "electronic media." The definition assumed that no transmissions made by voice via telephone existed in electronic form before transmission; the evolution of technology has made this assumption obsolete. This modification would extend the policy described in the preamble discussion quoted above, but correct its application to current technology, where some voice technology is digitally produced from an information system and transmitted by phone.

5. Definition of "Protected Health Information"

We propose to modify the definition of "protected health information" at § 160.103 to provide that the Privacy and Security Rules do not protect the individually identifiable health information of persons who have been deceased for more than 50 years. This proposed modification is explained more fully below in Section VI.E. of the preamble where we discuss the proposed changes to the Privacy Rule related to the protected health information of decedents.

6. Definition of "Respondent"

The definition of the term "Respondent," which is currently in § 160.302, would be moved to § 160.103. A reference to "business associate" would be added following the reference to "covered entity" in recognition of the potential liability imposed on business associates for violations of certain provisions of the Privacy and Security Rules by sections 13401 and 13404 of the Act.

7. Definition of "State"

The HITECH Act at section 13400, which became effective February 18, 2010, includes a definition of "State" to mean "each of the several States, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Northern Mariana Islands." This definition varies from paragraph (2) of the HIPAA definition of "State" at § 160.103, which does not include reference to American Samoa and the Northern Mariana Islands. Thus, for consistency with the definition applied to the HIPAA Rules by the HITECH Act, we propose to add reference to American Samoa and the Commonwealth of the Northern Mariana Islands in paragraph (2) of the definition of "State" at § 160.103.

8. Definition of "Workforce"

The HITECH Act is directly applicable to business associates and has extended liability for compliance with certain provisions of the Privacy and Security Rules to business associates. Because some provisions of the Act and the Privacy and Security Rules place obligations on the business associate with respect to workforce members, we propose to revise the definition of "workforce member" in § 160.103 to make clear that such term includes the employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a business associate, is under the direct control of the business associate.

D. Subpart B—Preemption of State Law, Section 160.201—Statutory Basis

We propose to modify § 160.201 regarding the statutory basis for the preemption of State law provisions to add a reference to section 264(c) of HIPAA, which contains the statutory basis for the exception to preemption at § 160.203(b) for State laws that are more stringent than the HIPAA Privacy Rule. We also propose to add a reference to section 13421(a) of the HITECH Act, which applies HIPAA's preemption rules to the HITECH Act's privacy and security provisions. Finally, we propose to re-title the provision to read "Statutory basis" instead of "Applicability."

We also take this opportunity to make clear that section 264(c)(2) of HIPAA and § 160.203(b) do not create a Federal evidentiary privilege. Additionally, we take this opportunity to make clear that neither the HIPAA statute nor its implementing regulations give effect to State physician-patient privilege laws or provisions of State law relating to the privacy of individually identifiable health information for use in Federal court proceedings. Therefore, consistent with the Supremacy Clause, any State law that was preempted prior to HIPAA because of conflicts with a Federal law would continue to be preempted. Nothing in HIPAA or its implementing regulations is intended to expand the

scope of State laws, regardless of whether they are more or less stringent than Federal law.

E. Subpart B—Preemption of State Law, Section 160.202—Definitions.

1. Definition of "Contrary"

The term "contrary" is currently defined in § 160.202 to make clear when the preemption provisions of HIPAA apply to State law. Consistent with the limited application of the HIPAA provisions to covered entities only, the current definition of the term "contrary" does not include reference to business associates. However, section 13421(a) of the HITECH Act provides that the HIPAA preemption provision (section 1178 of the Social Security Act) applies to the provisions and requirements under the HITECH Act "in the same manner" as it would apply under the HIPAA provisions. Thus, the preemption provisions would apply to business associates, who are now, by virtue of the HITECH Act, required to comply with certain provisions of the HIPAA Rules and are subject to penalties for noncompliance, as discussed elsewhere. Thus, we propose to amend the definition of "contrary" by inserting references to business associates in paragraph (1) of the definition. We also expand the reference to the HITECH statutory provisions in paragraph (2) of the definition to encompass all of the sections of subtitle D of the HITECH Act, rather than merely to section 13402, which was added by the breach notifications regulations. These changes would give effect to section 13421(a).

2. Definition of "More Stringent"

The term "more stringent" is part of the statutory preemption language under HIPAA. HIPAA preempts State law that is contrary to a HIPAA privacy standard unless, among other exceptions, the State law is more stringent than the contrary HIPAA privacy standard. The current regulatory definition of "more stringent" does not include business associates. We propose to amend the definition to add a reference to business associates, for the reasons set out in the preceding discussion.

IV. Section-by-Section Description of the Proposed Amendments to the Enforcement Rule—Subparts C and D of Part 160

Section 13410 of the HITECH Act made several amendments that directly impact the Enforcement Rule, which applies to the Secretary's enforcement of all of the HIPAA Administrative Simplification Rules, as well as the recently promulgated Breach Notification Rule. We issued an interim final rule on October 30, 2009, 74 FR 56123, to address the HITECH Act amendments impacting the Enforcement Rule that became effective on February 18, 2009. For context, we describe those modifications to the Enforcement Rule briefly below. We then provide a section-by-section description of the other section 13410 amendments that are part of this proposed rule.

In addition, sections 13401 and 13404 of the HITECH Act impose direct civil money penalty liability on business associates for violations of the HITECH Act and certain Privacy and Security Rule provisions. In doing so, sections 13401(b) and 13404(c) of the Act provide that section 1176 of the Social Security Act shall apply to a violation by a business associate "in the same manner" as it would apply to a covered entity with respect to such a violation. Both provisions are, by virtue of section 13423, effective February 18, 2010.

The provisions of subparts C and D of part 160 currently apply by their terms solely to covered entities. Accordingly, to implement sections 13401(b) and 13404(c) of the Act, we propose to revise a number of provisions in both subparts to reflect this statutory change by adding the term "business associate" where appropriate, following a reference to "covered entity." For ease, we list the sections in which the term "business associate" is added here rather than repeat the change in each discussion of the sections below: §§ 160.300; 160.304; 160.306(a) and (c); 160.308; 160.310; 160.312; 160.316; 160.401; 160.402; 160.404(b); 160.406; 160.408(c) and (d); and 160.410(a) and (c).

In addition to these references, we propose to add a paragraph in § 160.402(c)(2) to describe a business associate's liability for the actions of its agents, in accordance with the Federal common law of agency. This proposed modification is discussed more fully below in the discussion of § 160.402(c).

As noted above, the Department issued an interim final rule (IFR) on October 30, 2009, revising the Enforcement Rule to incorporate the provisions required by section 13410(d) of the HITECH Act that immediately took effect: Four categories of violations that reflect increasing levels of culpability, the corresponding tiers of civil money penalty amounts, and the revised limitations placed on the Secretary's authority to impose penalties. More specifically, the IFR revised subpart D of the Enforcement Rule to transfer the definitions of "reasonable cause," "reasonable diligence," and "willful neglect" from § 160.410(a) to a new definitions section at § 160.401. The IFR revised § 160.404 to incorporate, for violations occurring on or after February 18, 2009, the new penalty scheme required by section 13410(d), as follows: For violations in which it is established that the covered entity did not know and, by exercising reasonable diligence, would not have known that the covered entity violated a provision, an amount not less than $100 or more than $50,000 for each violation; for a violation in which it is established that the violation was due to reasonable cause and not to willful neglect, an amount not less than $1000 or more than $50,000 for each violation; for a violation in which it is established that the violation was due to willful neglect and was timely corrected, an amount not less than $10,000 or more than $50,000 for each violation; and for a violation in which it is established that the violation was due to willful neglect and was not timely corrected, an amount not less than $50,000 for each violation; except that a penalty for violations of the same requirement or prohibition under any of these categories may not exceed $1,500,000 in a calendar year. It also revised the affirmative defenses in § 160.410 for violations occurring on or after February 18, 2009, to remove a covered entity's lack of knowledge as an affirmative defense and to provide an affirmative defense when violations not due to willful neglect are corrected within 30 days. Finally, the IFR added a requirement that a notice of proposed determination pursuant to § 160.420 also reference the applicable category of violation. Readers are encouraged to refer to the IFR for a more detailed discussion of these topics as well as the Enforcement Rule's statutory and regulatory background. *See* 74 FR 56123, 56124, Oct. 30, 2009.

The rules proposed below would revise many provisions of subparts C and D of part 160. However, the Department's current interpretations of the regulatory provisions at subparts C and D continue unchanged, except to the extent they are inconsistent with the changes to those provisions, as indicated below.

A. Subpart C—Compliance and Investigations, Section 160.304—Principles for Achieving Compliance

Section 160.304 identifies cooperation and assistance as two overarching principles for achieving compliance. The principle of cooperation, in § 160.304(a), states that "[t]he Secretary will, to the extent practicable, seek the cooperation of covered entities in

obtaining compliance with the applicable administrative simplification provisions."

Section 13410(a) of the HITECH Act adds a new subsection (c) to section 1176 of the Social Security Act:

(c) NONCOMPLIANCE DUE TO WILLFUL NEGLECT.—

(1) IN GENERAL.—A violation of a provision of this part due to willful neglect is a violation for which the Secretary is required to impose a penalty under subsection (a)(1).

(2) REQUIRED INVESTIGATION.—For purposes of paragraph (1), the Secretary shall formally investigate any complaint of a violation of a provision of this part if a preliminary investigation of the facts of the complaint indicate such a possible violation due to willful neglect.

Section 13410(b)(1) makes the provisions of section 13410(a) effective February 18, 2011.

Under section 1176(c), HHS is required to impose a civil money penalty for violations due to willful neglect. Accordingly, although the Secretary often will still seek to correct indications of noncompliance through voluntary corrective action, there may be circumstances (such as circumstances indicating willful neglect), where the Secretary may seek to proceed directly to formal enforcement. As a conforming amendment, HHS proposes to add the phrase, "and consistent with the provisions of this subpart," to § 160.304(a) to recognize the statutory revision.

B. Subpart C—Compliance and Investigations, Section 160.306(c)—Complaints to the Secretary

Section 160.306(c) of the Enforcement Rule currently provides the Secretary with discretion to investigate HIPAA complaints, through use of the word "may." The new willful neglect provisions, at section 1176(c)(2) of the Social Security Act, will require HHS to investigate "any complaint of a violation of a provision of this part if a preliminary investigation of the facts of the complaint indicates * * * a possible violation due to willful neglect."

HHS proposes to implement section 1176(c)(2) by adding a new paragraph (1) at § 160.306(c) to provide that the Secretary *will* investigate any complaint filed under this section when a preliminary review of the facts indicates a possible violation due to willful neglect. As a practical matter, HHS currently conducts a preliminary review of every complaint received and proceeds with the investigation in every eligible case where its preliminary review of the facts indicate a possible violation of the HIPAA Rules. Nevertheless, we propose this addition to § 160.306 to make clear our intention to pursue an investigation where a preliminary review of the facts indicates a possible violation due to willful neglect.

HHS proposes to conform the remainder of § 160.306(c) accordingly. The new § 160.306(c)(2) (presently, the initial sentence of § 160.306(c)) would be revised by replacing "complaints" with "any other complaint" to distinguish the Secretary's discretion with respect to complaints for which HHS's preliminary review of the facts does not indicate a possible violation due to willful neglect from the statutory requirement to investigate *all* complaints for which HHS's preliminary review of the facts indicates a possible violation due to willful neglect, as set out in the new § 160.306(c)(1). The current second sentence of § 160.306(c), which addresses the content of an investigation, would be renumbered as § 160.306(c)(3) and amended by changing the first word of the sentence from "such" to "an," to signal the provision's application to any investigation, regardless of whether a preliminary review of the facts indicates a possible violation due to willful neglect.

C. Subpart C—Compliance and Investigations, Section 160.308—Compliance Reviews

Section 160.308 provides that the Secretary may conduct compliance reviews. Use of the word "may" in this section makes clear that this is a discretionary activity. While complaints and not compliance reviews are specifically mentioned in the statutory language of section 13410(a)(1)(B) of the Act regarding willful neglect, HHS proposes to also amend § 160.308 to provide that the Secretary will conduct a compliance review to determine whether a covered entity or business associate is complying with the applicable administrative simplification provision when a preliminary review of the facts indicates a possible violation due to willful neglect. This revision to § 160.308 furthers Congress' intent to strengthen enforcement with respect to potential violations due to willful neglect and ensures that investigations, whether or not initiated by complaint, are handled in a consistent manner. Also, the current language of § 160.308 would be redesignated as paragraph (b), and the words "in any other circumstance" would be added to the end of this paragraph to indicate that the discretionary authority of this paragraph applies to cases where the preliminary review of the facts does not indicate a possible violation due to willful neglect. Note that if HHS initiates an investigation of a complaint because its preliminary review of the facts indicates a possible violation due to willful neglect, HHS would not also be required to initiate a compliance review under this section, since it would be duplicative to do so.

D. Subpart C—Compliance and Investigations, Section 160.310—Responsibilities of Covered Entities

Section 160.310 explains a covered entity's responsibilities during complaint investigations and compliance reviews to make information available to the Secretary and to cooperate with the Secretary. Section 160.310(c)(3) provides that any protected health information obtained by the Secretary in connection with an investigation or compliance review will not be disclosed by the Secretary, except as necessary for determining and enforcing compliance with the HIPAA Rules or if otherwise required by law. We propose to also allow the Secretary to disclose protected health information if permitted under the Privacy Act at 5 U.S.C. 552a(b)(7). Section 552a(b)(7) permits the disclosure of a record on an individual contained within a Privacy Act protected system of records to another agency or instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law and if the agency has made a written request to the agency that maintains the record. This proposed change is necessary to permit the Secretary to cooperate with other law enforcement agencies, such as the State Attorneys General pursuing HIPAA actions on behalf of State residents pursuant to section 13410(e) of the Act, or the Federal Trade Commission, pursuing remedies under other consumer protection authorities.

E. Subpart C—Compliance and Investigations, Section 160.312—Secretarial Action Regarding Complaints and Compliance Reviews

Where noncompliance is indicated, § 160.312 requires the Secretary to attempt to resolve situations by informal means. Section 1176(c)(2) of the Social Security Act, as added by section 13410(a) of the HITECH Act, will require formal investigation of a complaint "if a preliminary investigation of the facts of the complaint indicate * * * a possible

violation due to willful neglect." Further, section 1176(c)(1) of the Social Security Act, as added by section 13410(a) of the HITECH Act, will require the Secretary to impose a civil money penalty where HHS makes a finding of a violation involving willful neglect. In addition to the proposed modification to § 160.306(c)(1), in light of the new provisions at section 1176(c), we propose to make clear that HHS is not required to attempt to resolve cases of noncompliance due to willful neglect by informal means. To do so, we propose to replace the word "will" in § 160.312(a)(1) with "may." While this change would permit HHS to proceed with a willful neglect determination as appropriate, it would also permit HHS to seek to resolve complaints and compliance reviews that did not indicate willful neglect by informal means (*e.g.,* where the covered entity or business associate did not know and by exercising reasonable diligence would not have known of a violation, or where the violation is due to reasonable cause).

It should be noted that this amendment would not change the substance of the response set forth in the April 18, 2005, preamble to the proposed Enforcement Rule, at 70 FR 20224, 20245–6, regarding objections to the 60-day time limit for filing a request for a hearing. In that response, HHS indicated that it was not reasonable to assume that a notice of proposed determination would be served on a respondent with no warning because the covered entity would necessarily be made aware of, and have the opportunity to address, HHS's compliance concerns throughout the investigative period preceding the notice of proposed determination. This proposed change to § 160.312 would allow the Secretary to proceed directly to a notice of proposed determination without first attempting to resolve the matter informally. This proposed revision does not change the fact that during the course of a complaint investigation or a compliance review, a covered entity or business associate would be made aware of, and have the opportunity to address, HHS's compliance concerns.

F. Subpart D—Imposition of Civil Money Penalties, Section 160.401—Definitions

Section 160.401 provides definitions of the terms "reasonable cause," "reasonable diligence," and "willful neglect." As discussed in the interim final rule, at 74 FR 56123, 56126–7, given section 13410(d) of the Act's use of these terms to describe the increasing levels of culpability for which increasing minimum levels of penalties may be imposed, HHS transferred these definitions from their prior placement at § 160.410(a) to signal the definitions' broader application to the entirety of subpart D of part 160. However, because section 13410(d) of the Act referred to these terms but did not amend these definitions, the interim final rule did not alter their content. HHS encourages readers, as it did in the interim final rule, to refer to prior preambles to the Enforcement Rule for detailed discussions of these terms at 70 FR 20224, 20237–9 and 71 FR 8390, 8409–11.

While the provisions of section 13410 of the Act do not explicitly require modification of these definitions, HHS is concerned that the *mens rea* demarcation between the categories of culpability associated with the new tiers of civil money penalty amounts is not sufficiently clear based on the existing definitions. As a result, certain violations (*i.e.,* those of which a covered entity or business associate has or should have knowledge, but does not have the conscious intent or reckless indifference associated with willful neglect) might not fit squarely within one of the established tiers. Therefore, HHS proposes to amend the definition of reasonable cause to clarify the scope of violations fitting within that definition.

HHS does not propose to otherwise modify the definitions associated with the categories of culpability of the amended section 1176(a) of the Social Security Act. However, we wish to clarify how the Secretary intends to apply these terms within this newly established context, to assist covered entities and business associates in tailoring their compliance activities appropriately. Accordingly, the discussion below also addresses the terms associated with the other categories of culpability (*i.e.,* knowledge, reasonable diligence, and willful neglect).

1. Reasonable Cause

Reasonable cause is currently defined, at § 160.401, to mean "circumstances that would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated." This definition is consistent with the Supreme Court's ruling in *United States* v. *Boyle,* 469 U.S. 241, 245 (1985), which focused on whether circumstances were beyond the regulated person's control, thereby making compliance unreasonable. *See* 70 FR 20224, 20238. Prior to the HITECH Act, section 1176 of the Social Security Act treated reasonable cause as a partial limitation on the Secretary's authority to impose a civil money penalty. That is, by establishing that a violation was due to reasonable cause and not willful neglect and was either corrected within a 30-day period or such additional period as the Secretary determined to be appropriate, a covered entity or business associate would bar the Secretary's imposition of a civil money penalty.

As described above, section 13410(d) of the HITECH Act revised section 1176 of the Social Security Act to establish four tiers of increasing penalty amounts to correspond to the levels of culpability associated with the violation. The first category of violation (and lowest penalty tier) covers situations where the covered entity or business associate did not know, and by exercising reasonable diligence would not have known, of a violation. The second category of violation (and next highest penalty tier) applies to violations due to reasonable cause and not to willful neglect. The third and fourth categories (and second-highest and highest penalty tiers) apply to circumstances where the violation was due to willful neglect that is corrected within a certain time period and willful neglect that is not so corrected, respectively. The importance of *mens rea,* or state of mind, in determining the degree of culpability is clear with respect to the first, third, and fourth categories, in that there is no *mens rea* with respect to the lowest category of violation, while the existence of *mens rea* is presumed with respect to the third and fourth categories of violation.

However, the current definition of reasonable cause does not address *mens rea* with respect to the second category of violations. HHS therefore proposes to amend the definition of "reasonable cause" in § 160.401 to clarify the full scope of violations that will come within the reasonable cause category of violations, including those circumstances that would make it unreasonable for the covered entity or business associate, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provisions violated, as well as those circumstances in which a covered entity or business associate has knowledge of a violation but lacks the conscious intent or reckless indifference associated with the willful neglect category of violations. To that end, HHS proposes to replace the current definition of "reasonable cause" with the following:

an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect.

As modified, the definition of "reasonable cause" will continue to recognize those circumstances that would make it unreasonable for the covered entity or business associate, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provisions violated. Consider the following example:

A covered entity received an individual's request for access but did not respond within the time periods provided for in § 164.524(b)(2). HHS's investigation reveals that the covered entity had compliant access policies and procedures in place, but that it had received an unusually high volume of requests for access within the time period in question. While the covered entity had responded to the majority of access requests received in that time period in a timely manner, it had failed to respond in a timely manner to several requests for access. The covered entity did respond in a timely manner to all requests for access it received subsequent to the time period in which the violations occurred.

In this example, the covered entity had knowledge of the violations but the investigation revealed circumstances that would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provisions violated. The investigation also revealed that the covered entity acted in a way that demonstrated a good faith attempt to comply with § 164.524(b)(2) by having compliant policies and procedures in place, responding to the majority of access requests in a timely manner, and otherwise responding to subsequent requests as required. In contrast, had the investigation revealed that the series of access requests occurred over a longer period of time, and that the covered entity did not attempt to address the backlog or communicate with the individuals, in writing, regarding the reasons for the delay or the date by which the covered entity would complete its action on the requests, the notice of proposed determination might alternatively categorize the violation as being due to willful neglect.

The modified definition of reasonable cause will also encompass those circumstances in which a covered entity or business associate has knowledge of the violation but lacks the conscious intent or reckless indifference associated with willful neglect. Consider the following example:

A covered entity presented an authorization form to a patient for signature to permit a disclosure for marketing purposes that did not contain the core elements required by § 164.508(c). HHS's investigation reveals that the covered entity was aware of the requirement for an authorization for a use or disclosure of protected health information for marketing and had attempted to draft a compliant authorization but had not included in the authorization the core elements required under § 164.508.

In this example, the covered entity failed to act with the ordinary care and business prudence of one seeking to comply with the Privacy Rule. Therefore, the violation cannot be considered to come within the category of violation that is associated with violations where the covered entity did not know (and by exercising reasonable diligence would not have known) of the violation. Yet, because the covered entity had attempted to draft a compliant authorization, it cannot be established that the omission was due to willful neglect involving either a conscious, intentional failure or reckless indifference to the obligation to comply with § 164.508. Unless otherwise resolved by informal means, HHS would have grounds to find that the violation was due to reasonable cause.

2. Knowledge and Reasonable Diligence

Prior rulemaking preambles discussing the Enforcement Rule explain the concept of knowledge, as it applies to the limitations (*i.e.,* affirmative defenses) that section 1176(b) of the Social Security Act places on the Secretary's authority to impose a civil money penalty. As they explain, "the knowledge involved must be knowledge that [a] violation has occurred, not just knowledge of the facts constituting the violation." *See* 71 FR 8390, 8410, Feb. 16, 2006. Moreover, a covered entity or business associate cannot assert an affirmative defense associated with its "lack of knowledge" if such lack of knowledge has resulted from its failure to inform itself about compliance obligations or to investigate received complaints or other information indicating likely noncompliance. *See* 70 FR 20224, 20237–8, Apr. 18, 2005 and 71 FR 8390, 8410–11, Feb. 16, 2006.

Section 13410(d) of the Act establishes the category of violations where the covered entity or business associate did not know (and by exercising reasonable diligence would not have known) of a violation as warranting the lowest range of civil money penalty amounts. The HITECH Act incorporated the concepts of knowledge and reasonable diligence from HIPAA, and it did not revise their substance. HHS therefore expects to apply these existing concepts to the newly established penalty structure consistent with its prior interpretations. Consider the following examples:

1. A covered health care provider with a direct treatment relationship with an individual patient failed to provide the patient a complete notice of privacy practices in compliance with § 164.520(c). HHS's investigation reveals that the covered entity has a compliant notice of privacy practices, policies and procedures for provision of the notice, and appropriate training of its workforce regarding the notice and its distribution. The violation resulted from a printing error that failed to print two pages of the notice of privacy practices. The printing error affected a small number of the covered entity's supply of notices and was an isolated failure to provide an individual with the covered entity's notice of privacy practices.

2. A business associate failed to terminate a former employee's access privileges to electronic protected health information in compliance with § 164.308(a)(3)(ii)(C). HHS's investigation reveals that the business associate's policies and procedures require the termination of such access within a reasonable time period. The HHS investigation reveals that the business associate attempted to terminate the former employee's access in accordance with its policy, but that it instead terminated the access of a current employee who had the same name as the former employee.

In both examples, HHS's investigations reveal that the covered entity or business associate has compliant policies and procedures in place, as well as some action by each covered entity or business associate indicating its intent to implement the respective Privacy Rule requirements. The investigations also reveal noncompliance that the exercise of reasonable diligence would not have avoided.

HHS also notes that, in some circumstances, we expect that the knowledge of an employee or agent of a covered entity or business associate may determine whether a violation implicates the "did not know" or "reasonable cause" categories of violation. That is, absent an exception under the Federal common law of agency, the knowledge of an employee or agent will generally be imputed to its principal (*i.e.,* the covered entity or business associate). *See* 70 FR 20224, 20237 and 71 FR 8390, 8402–3 (discussing imputation of knowledge under the Federal common law of agency and violations attributed to a covered entity, respectively). Consider the following example:

A hospital employee accessed the paper medical record of his ex-spouse while he was on duty to discover her current address for a personal reason, knowing that such access is not permitted by the Privacy Rule and contrary to the policies and procedures of the hospital. HHS's investigation reveals that the covered entity had appropriate and reasonable safeguards regarding employee access to medical records, and that it had delivered appropriate training to the employee.

In this example, the "did not know" category of violation is implicated with respect to the covered entity because the *mens rea* element of knowledge cannot be established. That is, while the employee's act is attributed to the covered entity, the employee's knowledge of the violation cannot be imputed to the covered entity because the employee was acting adversely to the covered entity. The Federal common law of agency does not permit the imputation of knowledge to the principal where the agent consciously acts in a manner that is adverse to the principal.

3. Willful Neglect

Willful neglect is defined, at § 160.401, to mean the "conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated." The term not only presumes actual or constructive knowledge on the part of the covered entity that a violation is virtually certain to occur but also encompasses a conscious intent or degree of recklessness with regard to its compliance obligations.

While the HITECH Act references willful neglect in several provisions, it does not revise the term's definition. HHS therefore expects to apply the current definition of willful neglect to all newly established contexts in the same manner as previously discussed. Consider the following examples:

1. A covered entity disposed of several hard drives containing electronic protected health information in an unsecured dumpster, in violation of § 164.530(c) and § 164.310(d)(2)(i). HHS's investigation reveals that the covered entity had failed to implement any policies and procedures to reasonably and appropriately safeguard protected health information during the disposal process.

2. A covered entity failed to respond to an individual's request that it restrict its uses and disclosures of protected health information about the individual. HHS's investigation reveals that the covered entity does not have any policies and procedures in place for consideration of the restriction requests it receives and refuses to accept any requests for restrictions from individual patients who inquire.

3. A covered entity's employee lost an unencrypted laptop that contained unsecured protected health information. HHS's investigation reveals the covered entity feared its reputation would be harmed if information about the incident became public and, therefore, decided not to provide notification as required by § 164.400 *et seq.*

The facts in these examples demonstrate that the covered entities had actual or constructive knowledge of their various violations. In addition, the covered entities' failures to develop or implement compliant policies and procedures or to respond to incidents as required by § 164.400 *et seq.* demonstrate either conscious intent or reckless disregard with respect to their compliance obligations. In the second example, the covered entity's refusal to accept any requests for restrictions from individual patients who inquire would be grounds for a separate finding of a violation due to willful neglect.

4. Correction of Willful Neglect Violations

We also note that while a covered entity's or business associate's correction of a willful neglect violation will not bar the imposition of a civil money penalty, such correction may foreclose the Secretary's authority to impose a penalty from the highest penalty tier prescribed by section 1176(a)(1) of the Social Security Act. While not all violations can be corrected, in the sense of being fully undone or remediated, HHS has previously set forth a broad interpretation of "corrected," in light of the statute's association of the term with "failure to comply." *See* 71 FR 8390, 8411 (recognizing that the term "corrected" could include correction of a covered entity's noncompliant procedure by making the procedure compliant). For example, in the event a covered entity's or business associate's inadequate safeguards policies and procedures result in an impermissible disclosure, the disclosure violation itself could not be fully undone or corrected. The safeguards violation, however, could be "corrected" in the sense that the noncompliant policies and procedures could be brought into compliance. In any event, corrective action will always be required of a covered entity or business associate.

G. Subpart D—Imposition of Civil Money Penalties, Section 160.402—Basis for a Civil Money Penalty

Section 160.402(a) provides the general rule that the Secretary will impose a civil money penalty upon a covered entity if the Secretary determines that the covered entity violated an administrative simplification provision. Paragraphs (b) and (c) of this section explain the basis for a civil money penalty against a covered entity where more than one covered entity is responsible for a violation, where an affiliated covered entity is responsible for a violation, and where an agent of a covered entity is responsible for a violation. As explained above, this proposed rule would add references to "business associate" where appropriate in this section to effectuate the HITECH Act's imposition of liability on business associates for violations of the HITECH Act and certain Privacy and Security Rule provisions.

Further, in paragraph (c), which provides the basis for the imposition of a civil money penalty against a covered entity for the acts of its agent, in accordance with the Federal common law of agency, we propose to add a parallel provision providing for civil money penalty liability against a business associate for the acts of its agent. Thus, we propose to add a new paragraph (2) to § 160.402(c) to provide that a business associate is liable, in accordance with the Federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the business associate, including a workforce member or subcontractor, acting within the scope of the agency.

The existing language of § 160.402(c) regarding the liability of covered entities for the acts of their agents would be redesignated as paragraph (1), with one substantive change. This section currently provides an exception for covered entity liability for the acts of its agent in cases where the agent is a business associate, the relevant contract requirements have been met, the covered entity did not know of a pattern or practice of the business associate in violation of the contract, and the covered entity did not fail to act as required by the Privacy or Security Rule with respect to such violations. We propose to remove this exception to principal liability for the covered entity so that the covered entity remains liable for the acts of its business associate agents, regardless of whether the covered entity has a compliant business associate agreement in place. This change is necessary to ensure, where the covered entity has contracted out a particular obligation under the HIPAA Rules, such as the requirement to provide individuals with a notice of privacy practices, that the covered entity remains liable for the failure of its business associate to perform that obligation on the covered entity's behalf.

We do not believe this proposed change would place any undue burden on covered entities, since covered entities are customarily liable for the acts of their agents under agency common law. We note that this proposed regulatory change does not create liability for covered entities with respect to business associates that are not agents, *e.g.,* independent contractors. The determination of whether a business associate is an agent of a covered entity, or whether a subcontractor is an agent of a business associate, will be based on the facts of the relationship, such as the level of control over the business associate's or subcontractor's conduct.

H. Subpart D—Imposition of Civil Money Penalties, Section 160.408—Factors Considered in Determining the Amount of a Civil Money Penalty

1. Determination of Penalty Amounts Prior to the HITECH Act

Section 160.408 implements section 1176(a)(2) of the Social Security Act, which requires the Secretary, when imposing a civil money penalty, to apply the provisions of section 1128A of the Social Security Act "in the same manner as such provisions apply to the imposition of a civil money penalty under section 1128A." As currently written, Section 1128A requires the Secretary to take into account—

(1) The nature of the claims and the circumstances under which they were presented,

(2) The degree of culpability, history of prior offenses and financial condition of the person presenting the claims, and

(3) Such other matters as justice may require.

Like other regulations that implement section 1128A, HHS tailored these factors by breaking them down into their component elements and providing a more specific list of circumstances, within each component, that apply to the context of HIPAA Rule violations. Because the Enforcement Rule applies to a number of rules, which apply to an enormous number of entities and circumstances, HHS left to the Secretary's discretion the decisions of whether and how (*i.e.,* as either aggravating or mitigating) to consider the following factors in determining the amount of a civil money penalty:

(a) The nature of the violation, in light of the purpose of the rule violated.

(b) The circumstances, including the consequences, of the violation, including but not limited to * * * [specific circumstances]

(c) The degree of culpability of the covered entity, including but not limited to * * * [specific circumstances]

(d) Any history of prior compliance with the administrative simplification provisions, including violations, by the covered entity, including but not limited to * * * [specific circumstances]

(e) The financial condition of the covered entity, including but not limited to * * * [specific circumstances]

(f) Such other matters as justice may require.

See 70 FR 20224, 20235–6 and 71 FR 8390, 8407–9 for a discussion of HHS's interpretation of the factors currently enumerated in § 160.408.

2. Determination of Penalty Amounts After the HITECH Act

As discussed in more detail in the IFR, section 13410(d) of the HITECH Act modified section 1176(a)(1) of the Social Security Act in several ways, including the establishment of tiers of penalty amounts that are associated with increasing levels of culpability. It also added a provision to section 1176(a)(1) of the Social Security Act directing HHS to "base such determination [of the appropriate penalty amount] on the nature and extent of the violation and the nature and extent of the harm resulting from such violation." The HITECH Act did not modify section 1176(a)(2) (requiring application of section 1128A). In addition, many of the factors currently identified by § 160.408 already pertain to the nature of the violation and the resulting harm. Section 160.408(a), for example, identifies the nature of the violation for consideration; paragraph (b) addresses the circumstances, including the consequences, of the violation (*e.g.,* physical harm, financial harm and whether the violation hindered or facilitated an individual's ability to obtain health care); and paragraph (f) addresses such other matters as justice may require. Thus, HHS did not modify § 160.408 in the IFR.

Upon further consideration of the statutory mandates and the significantly broader range of penalty amounts available, HHS believes it is appropriate to amend the structure of § 160.408, to make explicit the new statutory requirement that the Secretary consider the nature and extent of the violation and the nature and extent of the harm resulting from the violation, in addition to those factors enumerated in section 1128A. Thus, HHS proposes to revise § 160.408(a) and (b), as discussed below, to require the Secretary's consideration of the nature and extent of the violation, as well as the nature and extent of the harm resulting from violation, in addition to those factors referenced by section 1128A. We would exclude, however, the factor presently identified as § 160.408(c) (the degree of culpability of covered entity), which originated in section 1128A. Congress' revision of section 1176(a)(1) of the Social Security Act to establish increasing tiers of penalty amounts that reflect increasing degrees of culpability renders consideration of the degree of culpability as an aggravating or mitigating factor redundant. In contrast, HHS is not proposing to amend the Secretary's discretion with respect to the non-exhaustive list of specific circumstances that may be considered.

In addition, HHS proposes to reorganize the remaining, specific circumstances under § 160.408(a) and (b) to better reflect the categories to which they are now attributed, to add another circumstance for consideration under each, as described below, to explicitly provide that the Secretary's consideration of all specific circumstances is optional, and to modify the phrase "prior violations" in subsections (c)(1) and (2) to read "indications of noncompliance."

a. The Nature and Extent of the Violation

HHS proposes to revise subsection (a) to identify "[t]he nature and extent of the violation," as the first factor the Secretary must consider in determining a civil money penalty amount. While the "the nature of the violation" was previously identified for consideration, as it is grounded in section 1128A, the current list of factors in § 160.408 does not specifically reference "the extent of the violation," which section 1176(a) now requires. We also propose to transfer "the time period during which the violation(s) occurred," to this factor and to add, "the number of individuals affected," since both circumstances might be indicative measures of "the nature and extent of the violation." Our compliance and enforcement experience to date further supports the addition of the latter, particularly with respect to potential violations that negatively affect numerous individuals (*e.g.,* where disclosure of protected health information in multiple explanation of benefits statements that were mailed to the wrong individuals resulted from one inadequate safeguard but affected a large number of beneficiaries). We recognize these specific circumstances might also be considered under § 160.406, with respect to counting violations. In this regard, we direct readers' attention to 71 FR 8390, 8409 (responding to a comment expressing concern that the overlap of certain variables proposed in § 160.406 with factors proposed in § 160.408 might result in compound liability by asserting that since

consideration of such circumstances may be relevant to each separable element of the penalty calculation, their consideration will be different in nature).

b. The Nature and Extent of the Harm Resulting From the Violations

HHS proposes to revise subsection (a) to identify "[t]he nature and extent of the harm resulting from the violation" as the second factor the Secretary must consider. This minor amendment merely conforms the factor's language to the amended statutory language and continues to include the optional consideration of several specific circumstances which might be indicative of harm. In addition to these specific circumstances, HHS proposes to add reputational harm to make clear that reputational harm is as cognizable a form of harm as physical or financial harm.

c. The History of Prior Compliance With the Administrative Simplification Provisions

HHS proposes to modify the phrase "prior violations" in § 160.408(c)(1) and (2) to read "indications of noncompliance." As defined in § 160.302, "violation" or "violate" means, "as the context may require, failure to comply with an administrative simplification provision." Use of the term is generally reserved, however, to circumstances in which the Department has made a formal finding of a violation through a notice of proposed determination. As explained in 71 FR 8390, 8408, a covered entity's general history of HIPAA compliance is relevant in determining the amount of a civil money penalty within the penalty range. When we reviewed this language of § 160.408(c)(1) and (2) for the purposes of this rulemaking, we noticed that the regulatory text uses the term "violation" which is generally reserved for use in a notice of proposed determination. We are proposing to change this terminology to "indications of noncompliance" to make the regulatory language consistent with HHS' policy of considering a covered entity's general history of HIPAA compliance.

I. Section 160.410—Affirmative Defenses

Section 160.410 currently implements the limitations placed on the Secretary's authority to impose a civil money penalty under section 1176(b) of the Act. As amended by the IFR, § 160.410 is organized to implement section 13410(d) of the HITECH Act in a way that distinguishes the affirmative defenses available to covered entities and business associates prior to, on, or after February 18, 2009, the day after section 13410(d) of the HITECH Act became effective. *See* 74 FR 56123, Oct. 30, 2009, for a detailed discussion of the IFR's recent amendments.

Section 13410(a)(1) revises section 1176(b) to replace the phrase, "if the act constitutes an offense *punishable* under section 1177" with "a penalty *has been imposed* under section 1177 with respect to such act." This statutory change is effective February 18, 2011.

HHS proposes to amend § 160.410 to implement the revision of section 1176(b)(1) of the Social Security Act by providing in a new paragraph (a)(1) that the affirmative defense of criminally "punishable" is applicable to penalties imposed prior to February 18, 2011. A new paragraph (a)(2) in that section would make clear that, on or after February 18, 2011, the Secretary's authority to impose a civil money penalty will only be barred to the extent a covered entity or business associate can demonstrate that a penalty has been imposed under 42 U.S.C. 1320d–6 with respect to such act. As a conforming change, current paragraphs (a)(2) and (a)(3) are renumbered as paragraphs (b)(1) and (b)(2), respectively, and current paragraph (b) is renumbered as paragraph (c).

As an additional conforming change, HHS also proposes to amend § 160.410(a)(3)(i) (which has been redesignated as § 160.410(b)(2)(i)) to replace the term "reasonable cause" with the unrevised text of its current definition. This will ensure that the current definition is applied to violations occurring prior to February 18, 2009, thereby avoiding any potential issues regarding a retroactive application of the revised term.

J. Section 160.412—Waiver

We propose conforming changes to this section, to align the cross-references to § 160.410 with the proposed revisions to that section discussed above.

K. Subpart D—Imposition of Civil Money Penalties, Section 160.418—Penalty Not Exclusive

We propose to revise this section to incorporate a reference to the provision of the Patient Safety and Quality Improvement Act of 2005 at 42 U.S.C. 299b–22 that provides that penalties are not to be imposed under both that act and the Privacy Rule for the same violation.

V. Section-by-Section Description of the Proposed Amendments to Subpart A of Part 164 and the Security Rule in Subpart C of Part 164

The HITECH Act made several amendments that directly impact current provisions of the HIPAA Security Rule. We discuss the proposed changes to the Security Rule as a result of the HITECH Act in our section-by-section description below. We also discuss various technical and conforming proposed changes to the Security Rule, as well as proposed changes to provisions in subpart A of part 164, which applies to both the Security and Privacy Rules.

A. Technical Changes to Subpart A—General Provisions

1. Section 164.102—Statutory Basis

This section sets out the statutory basis of part 164. We propose a technical change to include a reference to the provisions of sections 13400 through 13424 of the HITECH Act upon which the regulatory changes proposed below are based.

2. Section 164.104—Applicability

This section sets out to whom part 164 applies. We propose to replace the existing paragraph (b) with an applicability statement for business associates, consistent with the provisions of the HITECH Act that are discussed more fully below. Proposed paragraph (b) would make clear that, where provided, the standards, requirements, and implementation specifications of the HIPAA Privacy, Security, and Breach Notification Rules apply to business associates. We propose to remove as unnecessary the existing language in § 164.104(b) regarding the obligation of a health care clearinghouse to comply with § 164.105 relating to organizational requirements of covered entities.

3. Section 164.105—Organizational Requirements

a. Section 164.105

Section 164.105 outlines the organizational requirements and implementation specifications for health care components of covered entities and for affiliated covered entities. As § 164.105 now also applies to subpart D of part 164 regarding breach notification for unsecured protected health information, we propose to remove several references to subparts C and E throughout this section to make clear that the provisions of this section also apply to the new subpart D of this part. In addition, we propose the following modifications to this section.

b. Section 164.105(a)(2)(ii)(C)–(E)

We propose to modify this section to remove as unnecessary paragraphs (C) and (D), which pertain to the obligation of a covered entity to ensure that any component that performs business associate-like activities and is included in the health care component complies with the requirements of the Privacy and Security Rules, and to re-designate paragraph (E) as (C). A covered entity's obligation to ensure that a health care component complies with the Privacy and Security Rules is already set out at § 164.105(a)(2)(ii). In addition, in light of a business associate's new direct liability for compliance with certain of the Security and Privacy Rule provisions, we request comment on whether we should require, rather than permit as is currently the case under § 164.105(a)(2)(iii)(C), a covered entity that is a hybrid entity to include a component that performs business associate-like activities within its health care component so that such components are directly subject to the Rules.

c. Section 164.105(a)(2)(iii)(C)

We propose to modify this section to re-designate § 164.105(a)(2)(iii)(C) as (D), and to include a new paragraph (C), which makes clear that, with respect to a hybrid entity, the covered entity itself, and not merely the health care component, remains responsible for complying with §§ 164.314 and 164.504 regarding business associate arrangements and other organizational requirements. This proposed modification is intended to recognize that hybrid entities may need to execute legal contracts and conduct other organizational matters at the level of the legal entity rather than at the level of the health care component.

d. Section 164.105(b)(1)

We propose to fix a minor typographical error in this paragraph by redesignating the second paragraph (1) as paragraph (2).

e. Section 164.105(b)(2)(ii)

We propose to simplify this paragraph by collapsing subparagraphs (A), (B), and (C) regarding the obligations of an affiliated entity to comply with the Privacy and Security Rules into one provision, and to expand the reference to compliance with the "part" so that the breach notification obligations in subpart D are also included.

4. Section 164.106—Relationship to Other Parts

We propose to add a reference to business associates, consistent with their inclusion elsewhere throughout the other HIPAA Rules.

B. Modifications to the HIPAA Security Rule in Subpart C

1. References to Business Associates

The Security Rule, as it presently stands, does not directly apply to business associates of covered entities. However, section 13401 of the HITECH Act, which became effective on February 18, 2010, provides that the Security Rule's administrative, physical, and technical safeguards requirements in §§ 164.308, 164.310, and 164.312, as well as its policies and procedures and documentation requirements in § 164.316, shall apply to business associates in the same manner as these requirements apply to covered entities, and that business associates shall be civilly and criminally liable for penalties for violations of these provisions.

Accordingly, to implement section 13401 of the HITECH Act, we propose to insert references to "business associate" in subpart C, as appropriate, following references to "covered entity" to make clear that these provisions of the Security Rule also apply to business associates. In particular, we propose to modify the following sections by adding references to business associates: §§ 164.302 (applicability), 164.304 (definitions of "administrative safeguard" and "physical safeguard"), 164.308, 164.310, 164.312, and 164.316. In addition, we propose the changes below to the Security Rule.

2. Section 164.306—Security Standards: General Rules

Section 13401 of the HITECH Act pertaining to requirements on business associates does not specifically make reference to § 164.306 of the Security Rule. However, § 164.306 sets out the general rules that apply to all of the security standards and implementation specifications that follow. Thus, for example, § 164.306(b)(2) sets out the particular factors that covered entities must take into account in deciding which security measures to use, and § 164.306(d) sets out the general rule that required implementation specifications must be implemented and the process and basis for implementing addressable implementation specifications. Accordingly, §§ 164.308, 164.310, and 164.312 provide that the administrative, physical, and technical safeguards of the Security Rule must be implemented "in accordance with § 164.306." We do not believe that Congress intended to apply enumerated Security Rule sections to business associates in a different manner than to covered entities, as evidenced by the statutory language that these sections should be applied to business associates "in the same manner that such sections apply to the covered entity." For these reasons, we also propose to revise § 164.306 to insert the word "business associate," as appropriate, so that the general rules found at § 164.306 apply to business associates in the same manner as covered entities.

In addition, we propose technical revisions to § 164.306(e) to more clearly indicate that to maintain security measures that continue to meet the requirements of §§ 164.308, 164.310, and 164.312, covered entities and business associates must review and modify such security measures and update documentation accordingly under § 164.316(b)(2)(iii).

3. Section 164.308—Administrative Safeguards

First, as noted above, we propose to modify § 164.308 to include throughout appropriate references to business associates. Second, we propose a technical change to § 164.308(a)(3)(ii)(C) regarding security termination procedures for workforce members, to add the words "or other arrangement with" after "employment of" in recognition of the fact that not all workforce members are employees (*e.g.,* some may be volunteers) of a covered entity or business associate. Third, we propose to remove the reference to § 164.306 in paragraph (b)(1) as unnecessary. Fourth, as discussed below, we propose a number of modifications to the provisions in this section regarding business associate contracts and other arrangements to conform to and address modifications proposed in the definition of "business associate," including the proposed inclusion of subcontractors within the scope of "business associate."

Section 164.308(b) provides that a covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information only if the covered entity has a contract or other arrangement in place to ensure the business associate will appropriately safeguard the protected health information. Section 164.308(b)(2) contains several exceptions to this general rule for certain situations that do not give rise to a business associate relationship, such as where a covered entity discloses electronic protected health information to a health care provider concerning the treatment of an individual. We propose to remove these exceptions from § 164.308(b)(2), since as discussed

above, we propose to include these as exceptions to the definition of "business associate."

In addition, we propose to modify § 164.308(b)(1) and (2) to clarify the new proposed requirements on business associates with regard to subcontractors. As described above with respect to the definition of "business associate" in § 160.103, we propose to include in the definition subcontractors that create, receive, maintain, or transmit protected health information on behalf of a business associate. However, we do not intend this proposed modification to mean that a covered entity is required to have a contract with the subcontractor. Rather, such obligation is to remain with the business associate who contracts with the subcontractor. Accordingly, in § 164.308(b)(1), we propose to clarify that covered entities are not required to obtain satisfactory assurances in the form of a contract or other arrangement with a business associate that is a subcontractor. In § 164.308(b)(2), we then propose to make clear that it is the business associate that must obtain the required satisfactory assurances from the subcontractor to protect the security of electronic protected health information.

We propose to remove the provision at § 164.308(b)(3), which provides that a covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the Security Rule's business associate provisions, as a covered entity's actions as a business associate of another covered entity are now directly regulated by the Security Rule's provisions that apply to business associates.

Finally, in § 164.308(b)(4) (renumbered as § 164.308(b)(3)), which requires documentation of the required satisfactory assurances through a written contract or other arrangement, we propose to add a reference to the new paragraph at § 164.308(b)(2) regarding business associates and subcontractors.

4. Section 164.314—Organizational Requirements

Section 13401 of the HITECH Act does not include § 164.314 among the provisions for which business associates are directly liable. However, section 13401 does state that § 164.308 applies to business associates "in the same manner" that the provision applies to covered entities. Section 164.308(b) requires a covered entity's business associate agreements to conform to the requirements of § 164.314. Accordingly, in order for § 164.308(b) to apply to business associates in the same manner as it applies to covered entities, we have revised § 164.314 to reflect that it is also applicable to agreements between business associates and subcontractors that create, receive, maintain, or transmit electronic protected health information.

We also propose a number of modifications to the business associate contract requirements in § 164.314 to streamline the provisions. First, we propose to remove § 164.314(a)(1)(ii) regarding the steps a covered entity must take if it knows of a material breach or violation by the business associate of the contract. A parallel provision exists in the Privacy Rule's business associate contract provisions at § 164.504 and, since a business associate for purposes of the Security Rule is also always a business associate for purposes of the Privacy Rule, the inclusion of a duplicate provision in the Security Rule is unnecessary. For the same reason, we also propose to remove the contract provision at § 164.314(a)(2)(i)(D) authorizing the termination of the contract by the covered entity if it is determined the business associate has violated a material term of the contract. A parallel provision exists in the Privacy Rule at § 164.504(e)(2)(iii). Also, because the Privacy Rule has a parallel provision, we remove the specific requirements under § 164.314(a)(2)(ii) for other arrangements, such as a memorandum of understanding when both a covered entity and business associate are governmental entities, and instead simply refer to the requirements of § 164.504(e)(3).

Second, we propose the following modifications to the remaining contract provision requirements: (1) In § 164.314(a)(2)(i)(A), we streamline the provision to simply indicate a business associate's obligation to comply with the Security Rule; (2) in § 164.314(a)(2)(i)(B), we revise the language with respect to ensuring subcontractors implement reasonable and appropriate safeguards to refer to the proposed requirement at § 164.308(b)(4) that would require a business associate to enter into a contract or other arrangement with a subcontractor to protect the security of electronic protected health information; and (3) in § 164.314(a)(2)(i)(C), with respect to the reporting of security incidents by business associates to covered entities, we make clear that the business associate contract must provide that the business associate will report to the covered entity breaches of unsecured protected health information as required by § 164.410 of the breach notification rules.

Third, we add a provision at § 164.314(a)(2)(iii) that provides that the requirements of this section for contracts or other arrangements between a covered entity and business associate would apply in the same manner to contracts or other arrangements between business associates and subcontractors required by the proposed requirements of § 164.308(b)(4). For example, to comply with proposed § 164.314(a)(2)(i)(C), a business associate contract between a business associate and a business associate subcontractor must provide that the subcontractor report any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410, to the business associate. Thus, if a breach of unsecured protected health information occurs at or by a subcontractor, the subcontractor must notify the business associate of the breach, which then must notify the covered entity of the breach. The covered entity then notifies the affected individuals, the Secretary, and, if applicable, the media, of the breach, unless it has delegated such responsibilities to a business associate.

Finally, we propose to remove the reference to subcontractors in § 164.314(b)(2)(iii) regarding amendment of group health plan documents as a condition of disclosure of protected health information to a plan sponsor, to avoid confusion with the use of the term subcontractor when referring to subcontractors that are business associates. This modification does not constitute a substantive change to § 164.314(b).

VI. Section-by-Section Description of the Proposed Amendments to the Privacy Rule

The HITECH Act made a number of amendments that affect current provisions of the Privacy Rule. In the section-by-section description of the proposed regulatory changes below, we discuss the HITECH Act requirements and the regulatory provisions affected by them, as well as certain other substantive proposed changes to the Privacy Rule intended to improve the workability and effectiveness of the Rule and to conform the Privacy Rule to PSQIA. At the end of this discussion, we also briefly list a number of proposed technical corrections and conforming changes to the Privacy Rule that are not otherwise addressed elsewhere.

A. Section 164.500—Applicability

We propose to revise § 164.500 to include new § 164.500(c) and to

redesignate the current § 164.500(c) as (d). In accordance with section 13404 of the HITECH Act, which applies certain of the Privacy Rule requirements to business associates, as discussed more fully below, § 164.500(c) would now clarify that, where provided, the standards, requirements, and implementation specifications of the Privacy Rule apply to business associates.

B. Section 164.501—Definitions

1. Definition of "Health Care Operations"

PSQIA, 42 U.S.C. 299b–21 *et seq.,* provides, among other things, that PSOs are to be treated as business associates of covered health care providers. Further, PSQIA provides that the patient safety activities of PSOs in relation to HIPAA covered health care providers are deemed to be health care operations under the Privacy Rule. *See* 42 U.S.C. 299b–22(i).

We propose to amend paragraph (1) of the definition of "health care operations" to include a reference to patient safety activities, as defined in the PSQIA implementing regulation at 42 CFR 3.20. Many health care providers participating in the voluntary patient safety program authorized by PSQIA are HIPAA covered entities; PSQIA acknowledges that such providers must also comply with the Privacy Rule and deems patient safety activities to be health care operations under the Privacy Rule. While such activities are already encompassed within paragraph (1) of the definition, which addresses various quality activities, we propose to expressly include patient safety activities within paragraph (1) of the definition of health care operations to expressly conform the definition to PSQIA and to eliminate the potential for any confusion. This modification would also address public comments the Department received during the rulemaking period for the PSQIA implementing regulations, which urged the Department to modify the definition of "health care operations" in the Privacy Rule to expressly reference patient safety activities so that the intersection of the Privacy and PSQIA Rules would be clear. *See* 73 FR 70732, 70780, November 21, 2008.

2. Definition of "Marketing"

The Privacy Rule requires covered entities to obtain a valid authorization from individuals before using or disclosing protected health information to market a product or service to them. *See* § 164.508(a)(3). Section 164.501 defines "marketing" as making a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. Paragraph (1) of the definition includes a number of exceptions to marketing for certain health-related communications. In particular, the Privacy Rule does not consider the following communications to be marketing: (1) Communications made 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 communications, including communications about: the entities participating in a healthcare 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; (2) communications made for the treatment of the individual; and (3) communications 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. Thus, a covered entity is permitted to make these excepted communications without an individual's authorization as either treatment or health care operations communications, as appropriate, under the Privacy Rule. In addition, the Privacy Rule does not require a covered entity to obtain individual authorization to communicate face-to-face or to provide only promotional gifts of nominal value to the individual. *See* § 164.508(a)(3)(i). However, a covered entity must obtain prior written authorization from an individual to send communications to the individual about non-health related products or services or to give or sell the individual's protected health information to a third party for marketing. *See* the current paragraph (2) of the definition of "marketing" in the Privacy Rule. Still, concerns have remained about the ability under these provisions for a third party to pay a covered entity in exchange for the covered entity to send health-related communications to an individual about the third party's products or services.

Section 13406(a) of the HITECH Act, which became effective on February 18, 2010, addresses these marketing provisions. In particular, section 13406(a) of the HITECH Act limits the health-related communications that may be considered health care operations and thus, that are excepted from the definition of "marketing" under the Privacy Rule to the extent a covered entity receives or has received direct or indirect payment in exchange for making the communication. In cases where the covered entity would receive such payment, the HITECH Act at section 13406(a)(2)(B) requires that the covered entity obtain the individual's valid authorization prior to making the communication, or, if applicable, prior to its business associate making the communication on its behalf in accordance with its written contract. Section 13406(a)(2)(A) of the HITECH Act includes an exception to the payment limitation for communications that describe only a drug or biologic that is currently being prescribed to the individual as long as any payment received by the covered entity in exchange for making the communication is reasonable in amount. Section 13406(a)(3) of the Act provides that the term "reasonable in amount" shall have the meaning given such term by the Secretary in regulation. Finally, section 13406(a)(4) of the Act clarifies that "direct or indirect payment" does not include any payment for treatment of the individual. We believe Congress intended with these provisions to curtail a covered entity's ability to use the exceptions to the definition of "marketing" in the Privacy Rule to send communications to the individual that were motivated more by commercial gain or other commercial purpose rather than for the purpose of the individual's health care, despite the communication's being about a health-related product or service.

To implement the marketing limitations of the HITECH Act, we propose a number of modifications to the definition of "marketing" in the Privacy Rule at § 164.501. In particular, we propose to: (1) Revise the exceptions to marketing to better distinguish the exceptions for treatment communications from those communications made for health care operations; (2) add a definition of "financial remuneration;" (3) provide that health care operations communications for which financial remuneration is received are marketing and require individual authorization; (4) provide that written treatment communications for which financial remuneration is received are subject to certain notice and opt out conditions set out at § 164.514(f)(2); (5) provide a limited exception from the remuneration prohibition for refill reminders; and (6) remove the paragraph regarding an arrangement between a covered entity and another

entity in which the covered entity receives remuneration in exchange for protected health information. We propose to revise §§ 164.514(f)(2) and 164.520(b)(1)(iii)(A) to include the notice and opt out conditions that would attach to written treatment communications about products or services sent by a health care provider to an individual in exchange for financial remuneration by the third party whose product or service is being described. We also propose to make a conforming change to the authorization requirements for marketing at § 164.508(a)(3)(ii). We describe these proposed modifications in more detail below.

In paragraph (1) of the definition of "marketing," we propose to maintain the general concept that "marketing" means "to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service." In paragraph (2) of the definition, we propose to include three exceptions to this definition to encompass certain treatment and health care operations communications about health-related products or services. First, at proposed paragraph (2)(iii), we would exclude from the definition of "marketing" certain health care operations communications, except where, as provided by section 13406(a)(2) of the HITECH Act, the covered entity receives financial remuneration in exchange for making the communication. This provision would encompass the health care operations activities currently described in paragraph (1)(i) of the definition of "marketing," which include communications 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. In addition, the provision would encompass health care operations communications for case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions, to the extent these activities do not fall within the definition of treatment. These are activities that currently fall within paragraph (1)(iii) of the definition of "marketing."

Although the HITECH Act uses the term "direct or indirect payment" to describe the limitation on permissible health care operations disclosures, we have substituted the term "financial remuneration" to avoid confusion since the Privacy Rule defines and uses the term "payment" to mean payment for health care and since the Privacy Rule's authorization requirements for marketing at § 164.508(a)(3) use the term "remuneration." We propose to define "financial remuneration" in paragraph (3) of the definition of "marketing" to mean direct or indirect payment from or on behalf of a third party whose product or service is being described. We also propose to make clear, in accordance with section 13406(a)(4) of the HITECH Act, that financial remuneration does not include any direct or indirect payment for the treatment of an individual. Additionally, because the HITECH Act refers expressly to "payment," rather than remuneration more generally, we have specified that only the receipt of financial remuneration in exchange for making a communication, as opposed to any other type of remuneration, is relevant for purposes of the definition of marketing. We propose a small conforming change to § 164.508(a)(3) to add the term "financial" before "remuneration" and to refer to the definition of "financial remuneration" for consistency with the HITECH Act and the proposed changes to the definition of "marketing."

We also emphasize that financial remuneration for purposes of the definition of "marketing" must be in exchange for making the communication itself and be from or on behalf of the entity whose product or service is being described. For example, authorization would be required prior to a covered entity making a communication to its patients regarding the acquisition of new state of the art medical equipment if the equipment manufacturer paid the covered entity to send the communication to its patients. In contrast, an authorization would not be required if a local charitable organization, such as a breast cancer foundation, funded the covered entity's mailing to patients about the availability of new state of the art medical equipment, such as mammography screening equipment, since the covered entity would not be receiving remuneration by or on behalf of the entity whose product or service was being described. Furthermore, it would not constitute marketing and no authorization would be required if a hospital sent flyers to its patients announcing the opening of a new wing where the funds for the new wing were donated by a third party, since the financial remuneration to the hospital from the third party was not in exchange for the mailing of the flyers.

Second, in paragraph (2)(ii) of the definition, we propose to include the statutory exception to marketing at section 13406(a)(2)(A) for communications regarding refill reminders or otherwise about a drug or biologic that is currently being prescribed for the individual, provided any financial remuneration received by the covered entity for making the communication is reasonably related to the covered entity's cost of making the communication. Congress expressly identified these types of communications as being exempt from the remuneration limitation only to the extent that any payment received for making the communication is reasonable in amount. We request comment on the scope of this exception, that is, whether communications about drugs that are related to the drug currently being prescribed, such as communications regarding generic alternatives or new formulations of the drug, should fall within the exception. In addition, we considered proposing a requirement that a covered entity could only receive financial remuneration for making such a communication to the extent it did not exceed the actual cost to make the communication. However, we were concerned that such a requirement would impose the additional burden of calculating the costs of making each communication. Instead, we propose to allow costs that are reasonably related to the covered entity's cost of making the communication. We request comment on the types and amount of costs that should be allowed under this provision.

Third, proposed paragraph (2)(i) would exclude from marketing treatment communications about health-related products or services by a health care provider to an individual, including communications 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, provided, however, that if the communications are in writing and financial remuneration is received in exchange for making the communications, certain notice and opt out conditions are met. We note that while section 13406(a) of the HITECH Act expressly provides that a communication to an individual about a health-related product or service where the covered entity receives payment from a third party in exchange for making the communication shall not be considered a *health care operation* (emphasis added) under the Privacy Rule, and thus is marketing, it is unclear how Congress intended these provisions to apply to treatment communications between a health care provider and a patient. Specifically, it is unclear whether Congress intended to restrict

only those subsidized communications about products and services that are less essential to an individual's health care (*i.e.,* those classified as health care operations communications) or all subsidized communications about products and services, including treatment communications. Given this ambiguity and to avoid preventing communications to the individual by a health care provider about health related products or services that are necessary for the treatment of the individual, we do not propose to require individual authorization where financial remuneration is received by the provider from a third party in exchange for sending the individual treatment communications about health-related products or services. However, to ensure the individual is aware that he or she may receive subsidized treatment communications from his or her provider and has the opportunity to elect not to receive them, we propose to require a statement in the notice of privacy practices when a provider intends to send such subsidized treatment communications to an individual, as well as the opportunity for the individual to opt out of receiving such communications. In particular, the proposed rule would exclude from marketing and the authorization requirements written subsidized treatment communications only to the extent that the following requirements proposed at § 164.514(f)(2) are met: (1) The covered health care provider's notice of privacy practices includes a statement informing individuals that the provider may send treatment communications to the individual concerning treatment alternatives or other health-related products or services where the provider receives financial remuneration from a third party in exchange for making the communication, and the individual has a right to opt out of receiving such communications; and (2) the treatment communication itself discloses the fact of remuneration and provides the individual with a clear and conspicuous opportunity to elect not to receive any further such communications. Similar to the modifications discussed below regarding fundraising communications, the opt out method provided to an individual for subsidized treatment communications may not cause the individual to incur an undue burden or more than a nominal cost. We encourage covered entities to consider the use of a toll-free phone number, an e-mail address, or similar opt out mechanism that would provide individuals with a simple, quick, and inexpensive way to opt out of receiving future communications. We note that we would consider requiring individuals to write and send a letter to the covered entity asking not to receive future communications to constitute an undue burden on the individual for purposes of this proposed requirement. We request comment on how the opt out should apply to future subsidized treatment communications. For example, we request comment on whether the opt out should prevent all future subsidized treatment communications by the provider or just those dealing with the particular product or service described in the current communication. We also request comment on the workability of requiring health care providers that intend to send subsidized treatment communications to individuals to provide an individual with the opportunity to opt out of receiving such communications prior to the individual receiving the first communication and what mechanisms could be put into place to implement the requirement.

Given that the new marketing limitations on the receipt of remuneration by a covered entity would apply differently depending on whether a communication is for treatment or health care operations purposes, it is important to emphasize the difference between the two types of communications. We note first that communications by health plans concerning health-related products or services included in a plan of benefits or for case management or care coordination are never considered treatment for purposes of the Privacy Rule but rather would always be health care operations and require individual authorization under the proposed rule if financial remuneration is involved. With respect to subsidized communications by a health care provider about health-related products or services for case management or care coordination or to recommend alternative treatments or settings of care, whether the communication would require individual authorization, or a statement in the notice and an opportunity to opt out, would depend on to what extent the provider is making the communication in a population-based fashion (health care operations) or to further the treatment of a particular individual based on that individual's health care status or condition (treatment). For example, a covered health care provider who sends a pregnant patient a brochure recommending a specific birthing center suited to the patient's particular needs is recommending a setting of care specific to the individual's condition, which constitutes treatment of the individual. If the health care provider receives financial remuneration in exchange for making the communication, the provider would be required to have included a statement in its notice of privacy practices informing individuals that it may send subsidized treatment communications to the individual and that the individual has a right to opt out of such communications, and to disclose the fact of remuneration with the communication and provide the individual with information on how to opt out of receiving future such communications. In contrast, a health care provider who sends a blanket mailing to all patients with information about a new affiliated physical therapy practice would not be making a treatment communication. Rather, the provider would be making a communication for health care operations if it does not receive any financial remuneration for the communication, but would be making a communication for marketing if it does receive financial remuneration.

We are aware of the difficulty in making what may be in some cases close judgments as to which communications are for treatment purposes and which are for health care operations purposes. We also are aware of the need to avoid unintended adverse consequences to a covered health care provider's ability to provide treatment to an individual. Therefore, we request comment on the above proposal with regard to these issues, as well as the alternatives of excluding treatment communications altogether even if they involve financial remuneration from a third party or requiring individual authorization for both treatment and health care operations communications made in exchange for financial remuneration.

We note that face to face communications about products or services between a covered entity and an individual and promotional gifts of nominal value provided by a covered entity are not impacted by these proposed changes to the definition of "marketing." These communications may continue to be made without obtaining an authorization under § 164.508 or meeting the notice and opt out requirements of § 164.514(f)(2). We also clarify that communications made by covered entities to individuals promoting health in general, such as communications about the importance of maintaining a healthy diet or getting an annual physical are still not considered to be marketing. These types

of communications do not constitute marketing because they are not promoting a specific product or service, and thus do not meet the definition of "marketing." Similarly, communications about government and government-sponsored programs do not fall within the definition of "marketing" as there is no commercial component to communications about benefits available through public programs.

Finally, we have proposed to remove the language at paragraph (2) from the definition of "marketing" at § 164.501. The current language defines as marketing an arrangement between a covered entity and any other entity in which the covered entity discloses protected health information to the other entity, in exchange for 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. This language describes a situation which, as explained more fully below, would now constitute a "sale" of protected health information under section 13405(d) of the HITECH Act and § 164.508(a)(4) of this proposed rule. Because we propose to modify § 164.508 to implement section 13405(d) of the HITECH Act by prohibiting the sale of protected health information without an authorization, we propose to remove this paragraph from the definition of "marketing" as unnecessary and to avoid confusion.

C. Business Associates

1. Section 164.502—Uses and Disclosures

The Privacy Rule currently does not directly govern business associates. However, the provisions of the HITECH Act make specific requirements of the Privacy Rule applicable to business associates, and create direct liability for noncompliance by business associates with regard to those Privacy Rule requirements. In particular, section 13404 of the HITECH Act, which became effective February 18, 2010, addresses the application of the provisions of the HIPAA Privacy Rule to business associates of covered entities. Section 13404(a) discusses the application of contract requirements to business associates, paragraph (b) applies the provision of § 164.504(e)(1)(ii) regarding knowledge of a pattern of activity or practice that constitutes a material breach or violation of a contract to business associates, and paragraph (c) applies the HIPAA civil and criminal penalties to business associates. We discuss paragraphs (a) and (b) of section 13404 of the HITECH Act below. We address section 13404(c) regarding the application of penalties to violations by business associates above in the discussion of the proposed changes to the Enforcement Rule.

Section 13404(a) of the HITECH Act creates direct liability for business associates by providing that in the case of a business associate of a covered entity that obtains or creates protected health information pursuant to a written contract or other arrangement as described in § 164.502(e)(2) of the Privacy Rule, the business associate may use and disclose such protected health information only if such use or disclosure is in compliance with the applicable business associate contract requirements of § 164.504(e) of the Rule. Additionally, section 13404(a) applies the other privacy requirements of the HITECH Act to business associates just as they apply to covered entities.

Accordingly, we propose to modify § 164.502(a) of the Privacy Rule containing the general rules for uses and disclosures of protected health information to address the permitted and required uses and disclosures of protected health information by business associates. First, we propose to revise § 164.502(a) to provide that a business associate, like a covered entity, may not use or disclose protected health information except as permitted or required by the Privacy Rule or the Enforcement Rule. Second, we propose to revise the titles of § 164.502(a)(1) and (2) regarding permitted and required uses and disclosures to make clear that these paragraphs apply only to covered entities. Note that in § 164.502(a)(2)(ii), we also propose a technical change to replace the term "subpart" with "subchapter" to make clear that a covered entity is required to disclose protected health information to the Secretary as needed to determine compliance with any of the HIPAA Rules and not just the Privacy Rule.

Third, we propose to add new provisions at § 164.502(a)(4) and (5) to address the permitted and required uses and disclosures of protected health information by business associates.[4] In accordance with section 13404(a) of the HITECH Act, proposed § 164.502(a)(4) would allow business associates to use or disclose protected health information only as permitted or required by their business associate contracts or other arrangements pursuant to § 164.504(e), or as required by law. If a covered entity and business associate have failed to enter into a business associate contract or other arrangement, then the business associate may use or disclose protected health information only as necessary to perform its obligations for the covered entity (pursuant to whatever agreement sets the general terms for the relationship between the covered entity and business associate) or as required by law; any other use or disclosure would violate the Privacy Rule. In addition, proposed § 164.502(a)(4) makes clear that a business associate would not be permitted to use or disclose protected health information in a manner that would violate the requirements of the Privacy Rule, if done by the covered entity, except that the business associate would be permitted to use or disclose protected health information for the purposes specified under § 164.504(e)(2)(i)(A) or (B), pertaining to uses and disclosures for the proper management and administration of the business associate and the provision of data aggregation services for the covered entity, if such uses and disclosures are permitted by its business associate contract or other arrangement.

Section 164.502(a)(5) would require business associates to disclose protected health information either when required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the business associate's compliance with this subchapter, or to the covered entity, individual, or individual's designee, as necessary to satisfy a covered entity's obligations under § 164.524(c)(2)(ii) and (3)(ii), as modified, with respect to an individual's request for an electronic copy of protected health information. As section 13405(e) requires covered entities that maintain protected health information in an electronic health record to provide an individual, or the individual's designee, with a copy of such information in an electronic format, if the individual so chooses, and as section 13404(a) applies section 13405(e) to business associates as well, we propose to include such language in § 164.502(a)(5).

We propose to modify the minimum necessary standard at § 164.502(b) to require that when business associates use, disclose, or request protected health information, they limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. Applying the minimum necessary standard is a condition of the permissibility of many uses and disclosures of protected health information. Thus, a business associate

[4] We propose to reserve § 164.502(a)(3) for provisions implementing modifications to the Privacy Rule required by the Genetic Information Nondiscrimination Act of 2008 (GINA), which were proposed on October 7, 2009. *See* 74 FR 51698.

is not making a permitted use or disclosure under the Privacy Rule if it does not apply the minimum necessary standard, where appropriate. Additionally, the HITECH Act at section 13405(b) addresses the application of minimum necessary and, in accordance with section 13404(a), also applies such requirements to business associates. We note that we have not added references to "business associate" to other provisions of the Privacy Rule that address uses and disclosures by covered entities. This is because we found such changes to be unnecessary, since a business associate generally may only use or disclose protected health information in the same manner as a covered entity (therefore any Privacy Rule limitation on how a covered entity may use or disclose protected health information automatically extends to business associates).

Section 164.502(e) sets out the requirements for disclosures to business associates. We propose in § 164.502(e)(1)(i) to provide that covered entities are not required to obtain satisfactory assurances from business associates that are subcontractors. Rather, as we previously discussed with regard to proposed modifications to the Security Rule pertaining to business associates, and as we discuss further below, we propose in the Privacy and Security Rules to require that business associates obtain satisfactory assurances, through a written contract or other arrangement, from subcontractors that provide that the subcontractor will comply with the applicable requirements of the Rules. Accordingly, each business associate subcontractor would be subject to the terms and conditions of a business associate agreement with a business associate, eliminating the need for a similar agreement with the covered entity itself.

We also propose to move the current exceptions to business associates at § 164.502(e)(1)(ii) to the revised definition of business associates found in § 160.103 for the reasons discussed in that section.

We propose a new § 164.502(e)(1)(ii) that provides that a business associate may disclose protected health information to a business associate that is a subcontractor, and to allow the subcontractor to create or receive protected health information on behalf of the business associate, if the business associate obtains satisfactory assurances, in accordance with § 164.504(e)(1)(i), that the subcontractor will appropriately safeguard the information. As such, the business associate must enter into a contract or other arrangement that complies with § 164.504(e)(1)(i) with business associate subcontractors, in the same manner that covered entities are required to enter into contracts or other arrangements with their business associates. As we discussed with regard to the requirements of the Security Rule regarding business associates, we believe that business associates are in the best position to ensure that subcontractors comply with the requirements of the Privacy Rule. For example, a covered entity may choose to contract with a business associate (contractor) to use or disclose protected health information on its behalf, the business associate may choose to obtain the services of (and exchange protected health information with) a subcontractor (subcontractor 1), and that subcontractor may, in turn, contract with another subcontractor (subcontractor 2) for services involving protected health information. Under the current rules, the covered entity would be required to obtain a business associate agreement with the contractor, the contractor would have a contractual requirement to obtain the same satisfactory assurances from subcontractor 1, and subcontractor 1 would in turn have a contractual requirement to obtain the same satisfactory assurances from subcontractor 2. The proposed revisions to the Privacy and Security Rules would not change the parties to the contracts. However, the contractor and subcontractors 1 and 2 all would now be business associates with direct liability under the HIPAA Rules, and would be required to obtain business associate agreements with the parties with whom they contract for services that involve access to protected health information. (*Note,* however, as discussed above with respect to the definition of "business associate," direct liability under the HIPAA Rules attaches regardless of whether the contractor and subcontractors have entered into business associate agreements.) The proposed revisions ensure that the covered entity does not have a new obligation to enter into separate contracts with the business associate subcontractors.

We propose to remove § 164.502(e)(1)(iii), which provides that a covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the Privacy Rule's business associate provisions, given that new proposed § 164.502(a)(4) would restrict directly the uses and disclosures of protected health information by a business associate, including a covered entity acting as a business associate, to those uses and disclosures permitted by its business associate agreement.

2. Section 164.504(e)—Business Associate Agreements

Section 164.504, among other provisions, contains the specific requirements for business associate contracts and other arrangements. As discussed previously, section 13404 of the HITECH Act provides that a business associate may use and disclose protected health information only if such use or disclosure is in compliance with each applicable requirement of § 164.504(e), and also applies the provisions of § 164.504(e)(1)(ii), which outline the actions that must be taken if the business associate has knowledge of a breach of the contract, to business associates. We propose a number of modifications to this section to implement these provisions and to reflect the Department's new regulatory authority with respect to business associates, as well as to reflect a covered entity's and business associate's new obligations under subpart D to provide for notification in the case of breaches of unsecured protected health information.

Section 164.504(e)(1)(ii) provides that a covered entity is not in compliance with the business associate requirements if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and if such steps were unsuccessful, terminated the contract or arrangement or, if termination is not feasible, reported the problem to the Secretary. We propose to revise § 164.504(e)(1)(ii) to remove the requirement that covered entities report to the Secretary when termination of a business associate contract is not feasible. In light of a business associate's direct liability for civil money penalties for violations of the HIPAA Rules and both a covered entity's and business associate's obligations under subpart D to report breaches of unsecured protected health information to the Secretary, we have other mechanisms through which we expect to learn of such breaches and misuses of protected health information by a business associate. We also propose to add a new provision at § 164.504(e)(1)(iii) applicable to business associates with respect to subcontractors to mirror the requirements on covered entities in

§ 164.504(e)(1)(ii) (minus the requirement to report to the Secretary if termination of a contract is not feasible). Thus, proposed § 164.504(e)(1)(iii) would require a business associate, if it knew of a pattern or practice of activity of its business associate subcontractor that constituted a material breach or violation of the subcontractor's contract or other arrangement, to take reasonable steps to cure the breach of the subcontractor or to terminate the contract, if feasible. We believe this proposed provision would implement the intent of section 13404(b) of the HITECH Act, and aligns the requirements for business associates with regard to business associate subcontractors with the requirements for covered entities with regard to their business associates. In other words, a business associate that is aware of noncompliance by its business associate subcontractor must respond to the situation in the same manner as a covered entity that is aware of noncompliance by its business associate.

While business associates are now directly liable for civil money penalties under the HIPAA Rules for impermissible uses and disclosures as described above, business associates are still contractually liable to covered entities pursuant to their business associate contracts, as provided for and required by § 164.504(e). We propose certain modifications to these contract requirements. First, we propose to revise § 164.504(e)(2)(ii)(B) through (D) to require the following: in (B), that business associates comply, where applicable, with the Security Rule with regard to electronic protected health information; in (C), that business associates report breaches of unsecured protected health information to covered entities, as required by § 164.410; and in (D), that, in accordance with § 164.502(e)(1)(ii), business associates ensure that any subcontractors that create or receive protected health information on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information. These proposed revisions align the requirements for the business associate contract with the requirements in the HITECH Act and elsewhere within the HIPAA Rules.

Additionally with regard to business associate contract requirements, we propose to insert a new provision at § 164.502(e)(2)(ii)(H) and to renumber the current paragraphs (H) and (I) accordingly. Section 164.502(e)(2)(ii)(H), as proposed, would require that, to the extent the business associate is to carry out a covered entity's obligation under this subpart, the business associate must comply with the requirements of the Privacy Rule that apply to the covered entity in the performance of such obligation. The HITECH Act places direct liability for uses and disclosures and for the other HITECH Act requirements on business associates. Beyond such direct liability, this provision clarifies that a business associate is contractually liable not only for uses and disclosures of protected health information, but also for all other requirements of the Privacy Rule, as they pertain to the performance of the business associate's contract. For example, if a third party administrator, as a business associate of a group health plan, fails to distribute the plan's notice of privacy practices to participants on a timely basis, the third party administrator would not be directly liable under the HIPAA Rules, but would be contractually liable, for the failure. However, we emphasize that in this example, even though the business associate is not directly liable under the HIPAA Rules for failure to provide the notice, the covered entity remains directly liable for failure to provide the individuals with its notice of privacy practices because it is the covered entity's ultimate responsibility to do so, despite its having hired a business associate to perform the function.

We also propose to revise § 164.504(e)(3) regarding other arrangements for governmental entities to include references to the Security Rule requirements for business associates to streamline the two rules and, as discussed above, to avoid having to repeat such provisions in the Security Rule.

To implement the requirements of sections 13404(a) of the HITECH Act, we propose to include a new § 164.504(e)(5) that applies the requirements of § 164.504(e)(2) through (e)(4) to the contract or other arrangement between a business associate and its business associate subcontractor as required by § 164.502(e)(1)(ii) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and its business associate. As such, the business associate is required by § 164.502(e)(1)(ii) and by this section to enter into business associate contracts, or other arrangements that comply with the Privacy and Security Rules, with their business associate subcontractors in the same manner that covered entities are required to enter into contracts or other arrangements with their business associates.

Finally, we propose to remove the reference to subcontractors in § 164.504(f)(2)(ii)(B) to avoid confusion with the use of the term subcontractor when referring to subcontractors as business associates. For the same reason, we propose to remove the reference to subcontractors in § 164.514(e)(4)(ii)(C)(4) to avoid confusion with the use of the term subcontractor when referring to subcontractors as business associates. We do not intend these proposed modifications to constitute substantive changes.

3. Section 164.532—Transition Provisions

We understand that covered entities and business associates are concerned with the anticipated administrative burden and cost to implement the revised business associate contract provisions of the Privacy and Security Rules. Covered entities may have existing contracts that are not set to terminate or expire until after the compliance date of the modifications to the Rules, and we understand that a six month compliance period may not provide enough time to reopen and renegotiate all contracts. In response to these concerns, we propose to relieve some of the burden on covered entities and business associates in complying with the revised business associate provisions by adding a transition provision to grandfather certain existing contracts for a specified period of time. The Department's authority to add the transition provision is set forth in § 160.104(c), which allows the Secretary to establish the compliance date for any modified standard or implementation specification, taking into account the extent of the modification and the time needed to comply with the modification. We also note that the Final Privacy Rule, 65 FR 82462 (Dec. 28, 2000), and the Modifications to the HIPAA Privacy Rule, 67 FR 53182 (Aug. 14, 2002), both included transition provisions to ensure that important functions of the health care system were not impeded (*e.g.,* to prevent disruption of ongoing research). Similarly, the proposed transition period, here, will prevent rushed and hasty changes to thousands of on-going existing business associate agreements. The following discussion addresses the issue of the business associate transition provisions.

We propose new transition provisions at § 164.532(d) and (e) to allow covered entities and business associates (and business associates and business associate subcontractors) to continue to operate under certain existing contracts for up to one year beyond the

compliance date of the revisions to the Rules. The additional transition period would be available to a covered entity or business associate if, prior to the publication date of the modified Rules, the covered entity or business associate had an existing contract or other written arrangement with a business associate or subcontractor, respectively, that complied with the prior provisions of the HIPAA Rules and such contract or arrangement was not renewed or modified between the effective date and the compliance date of the modifications to the Rules. The proposed provisions are intended to allow those covered entities and business associates with contracts with business associates and subcontractors, respectively, that qualify as described above to continue to disclose protected health information to the business associate or subcontractor, or to allow the business associate or subcontractor to create or receive protected health information on behalf of the covered entity or business associate, for up to one year beyond the compliance date of the modifications, regardless of whether the contract meets the applicable contract requirements in the modifications to the Rules. With respect to business associates and subcontractors, this proposal would grandfather existing written agreements between business associates and subcontractors entered into pursuant to 45 CFR 164.504(e)(2)(i)(D), which requires the business associate to ensure that its agents with access to protected health information agree to the same restrictions and conditions that apply to the business associate. The Department proposes to deem such contracts to be compliant with the modifications to the Rules until either the covered entity or business associate has renewed or modified the contract following the compliance date of the modifications, or until the date that is one year after the compliance date, whichever is sooner.

In cases where a contract renews automatically without any change in terms or other action by the parties (also known as "evergreen contracts"), the Department intends that such evergreen contracts will be eligible for the extension and that deemed compliance would not terminate when these contracts automatically roll over. These transition provisions apply to covered entities and business associates only with respect to written contracts or other written arrangements as specified above, and not to oral contracts or other arrangements.

These transition provisions only apply to the requirement to amend contracts; they do not affect any other compliance obligations under the HIPAA Rules. For example, beginning on the compliance date of this rule, a business associate may not use or disclose protected health information in a manner that is contrary to the Privacy Rule, even if the business associate's contract with the covered entity has not yet been amended.

D. Section 164.508—Uses and Disclosures for Which an Authorization is Required

Section 164.508 of the Privacy Rule permits a covered entity to use and disclose protected health information only if it has obtained a valid authorization (*i.e.,* one that meets the requirements of the section), unless such use or disclosure is otherwise permitted or required by the Privacy Rule. Section 164.508 also lists two specific circumstances in which an authorization must be obtained: (1) Most uses and disclosures of psychotherapy notes; and (2) uses and disclosures for marketing.

1. Sale of Protected Health Information

Section 13405(d) of the HITECH Act adds a third circumstance that requires authorization, specifically the sale of protected health information. Section 13405(d)(1) prohibits a covered entity or business associate from receiving direct or indirect remuneration in exchange for the disclosure of protected health information unless the covered entity has obtained a valid authorization from the individual pursuant to § 164.508 that states whether the protected health information can be further exchanged for remuneration by the entity receiving the information. Section 13405(d)(2) sets forth several exceptions to the authorization requirement. These exceptions are where the purpose of the exchange of information for remuneration is for: (1) Public health activities, as described in § 164.512(b); (2) research purposes as described in §§ 164.501 and 164.512(i), if the price charged for the information reflects the costs of preparation and transmittal of the data; (3) treatment of the individual; (4) the sale, transfer, merger, or consolidation of all or part of a covered entity and for related due diligence; (5) services rendered by a business associate pursuant to a business associate agreement and at the specific request of the covered entity; (6) providing an individual with access to his or her protected health information pursuant to § 164.524; and (7) such other purposes as the Secretary determines to be necessary and appropriate by regulation. Section 13405(d)(4) of the Act provides that the prohibition on sale of protected health information shall apply to disclosures occurring 6 months after the date of the promulgation of final regulations implementing this section.

To implement section 13405(d) of the HITECH Act, we propose to add new provisions at § 164.508(a)(4) regarding the sale of protected health information. In proposed § 164.508(a)(4)(i), we propose to require a covered entity to obtain an authorization for any disclosure of protected health information in exchange for direct or indirect remuneration. This authorization must state that the disclosure will result in remuneration to the covered entity. In proposed § 164.508(a)(4)(ii), we propose to except several disclosures of protected health information, made in exchange for remuneration, from this authorization requirement. These exceptions, as discussed more fully below, generally follow the statutory exceptions described in the above paragraph.

The proposed language in § 164.508(a)(4)(i) generally follows the statutory language of section 13405(d)(1) in prohibiting the disclosure of protected health information without an authorization if the covered entity receives direct or indirect remuneration from or on behalf of the recipient of the protected health information. As required by the Act, this proposed provision would apply to business associates as well as to covered entities.

We do not include language in proposed § 164.508(a)(4) to require that the authorization under § 164.508 specify whether the protected health information disclosed by the covered entity for remuneration can be further exchanged for remuneration by the entity receiving the information. We believe the intent of this statutory language was to ensure that, as currently required by § 164.508 for marketing, the authorization include a statement as to whether remuneration will be received by the covered entity with respect to the disclosures subject to the authorization. Otherwise, the individual would not be put on notice that the disclosure involves remuneration and thus, would not be making an informed decision as to whether to sign the authorization. Accordingly, we propose to require that the § 164.508(a)(4)(i) authorization include a statement that the covered entity is receiving direct or indirect remuneration in exchange for the protected health information. This requirement would ensure that individuals can make informed decisions regarding whether to authorize disclosure of their protected health information when the disclosure

will result in remuneration to the covered entity. We also note, with respect to the recipient of the information, if protected health information is disclosed for remuneration by a covered entity or business associate to another covered entity or business associate in compliance with the authorization requirements at proposed § 164.508(a)(4)(i), the recipient covered entity or business associate could not redisclose that protected health information in exchange for remuneration unless a valid authorization is obtained in accordance with proposed § 164.508(a)(4)(i) with respect to such redisclosure. We request comment on these provisions.

In proposed § 164.508(a)(4)(ii), we set forth the exceptions to the authorization requirement of proposed paragraph (a)(4)(i). We propose the exceptions provided for by section 13405(d)(2) of the HITECH Act, but we also propose to exercise the authority granted to the Secretary in section 13405(d)(2)(G) to include an additional exception that we deem to be similarly necessary and appropriate. We invite public comment on the proposed exceptions to this authorization requirement and whether there are additional exceptions that should be included in the final regulation.

The exception at proposed § 164.508(a)(4)(ii)(A) covers exchanges for remuneration for public health activities pursuant to §§ 164.512(b) or 164.514(e). This exception largely tracks the statutory language; however, we have added a reference to § 164.514(e), to ensure that a covered entity or business associate that discloses protected health information for public health activities in limited data set form is also excepted from the authorization requirement. We believe it is consistent with the statutory language to also except the disclosure of a limited data set where Congress has already excepted the disclosure of fully identifiable protected health information for the same purpose from the remuneration prohibition. With respect to the exception for public health disclosures, section 13405(d)(3)(A) of the HITECH Act requires that the Secretary evaluate the impact of restricting this exception to require that the price charged for the data reflects only the costs of preparation and transmittal of the data on research or public health activities, including those conducted by or for the use of the Food and Drug Administration (FDA). Section 13405(d)(3)(B) further provides that if the Secretary finds that such further restriction will not impede such activities, the Secretary may include the restriction in the regulations. While we do not propose to include such a restriction on the remuneration that may be received for disclosures for public health purposes at this time, we request public comment on this issue to assist us in evaluating the impact of any such restriction.

The proposed exception at § 164.508(a)(4)(ii)(B) generally tracks the statutory language and excepts from the authorization requirement disclosures of protected health information for research purposes, pursuant to §§ 164.512(i) or 164.514(e), in which the covered entity receives remuneration, as long as the remuneration received by the covered entity is a reasonable, cost-based fee to cover the cost to prepare and transmit the information for research purposes. We request public comment on the types of costs that should be permitted under this provision. As discussed above with respect to the exception for public health activities, we also propose to add a reference to § 164.514(e) to ensure that this exception likewise applies to the disclosure of protected health information in limited data set form for research purposes.

Proposed § 164.508(a)(4)(ii)(C) would create an exception from the authorization requirement for disclosures of protected health information for treatment and payment purposes, in which the covered entity receives remuneration. Though the Act only addressed treatment, we have expressly included disclosures for payment purposes and have also included reference to § 164.506(a), which sets forth the standard for disclosures of protected health information for treatment and payment purposes. We also propose to except disclosures made for payment for health care from the remuneration limitation to make clear that we do not consider the exchange of protected health information to obtain "payment," as such term is defined in the Privacy Rule at § 164.501, to be a sale of protected health information and thus, subject to the authorization requirements in this section.

Section 13405(d)(2)(D) of the HITECH Act excepts from the authorization requirement disclosures described in paragraph (6)(iv) of the definition of health care operations at § 164.501, *i.e.,* disclosures for the sale, transfer, merger, or consolidation of all or part of a covered entity with another covered entity, or an entity that following such activity will become a covered entity, and due diligence related to such activity. Proposed § 164.508(a)(4)(ii)(D) would accordingly except from the authorization requirement disclosures of protected health information for the events described in paragraph (6)(iv). We also add a reference to § 164.506(a), the provision which permits a covered entity to disclose protected health information for health care operations purposes.

Proposed § 164.508(a)(4)(ii)(E) would except from the authorization requirements disclosures of protected health information to or by a business associate for activities that the business associate undertakes on behalf of a covered entity pursuant to §§ 164.502(e) and 164.504(e), as long as the only remuneration provided is by the covered entity to the business associate for the performance of such activities. We have modified the statutory language to provide specific references to the provisions of the Privacy Rule that set forth the standards through which covered entities may make disclosures of protected health information to business associates and the standards for business associate contracts which govern the relationship between covered entities and their business associates. This proposed exception would exempt from the authorization requirement in § 164.508(a)(4)(i) a disclosure of protected health information by a covered entity to a business associate or by a business associate to a third party on behalf of the covered entity as long as any remuneration received by the business associate was for payment for the activities performed by the business associate pursuant to a business associate contract.

Proposed § 164.508(a)(4)(ii)(F) would except from the authorization requirement disclosures of protected health information by a covered entity to an individual when requested under §§ 164.524 or 164.528. While section 13405(d)(2)(F) explicitly refers only to disclosures under § 164.524, we are exercising our authority under section 13405(d)(2)(G) of the HITECH Act (discussed below) to include in this proposed section disclosures under § 164.528 as necessary and appropriate. Section 164.502(a)(2)(i) requires covered entities to disclose protected health information relating to an individual to that individual upon request pursuant to §§ 164.524 or 164.528. Section 164.524 permits a covered entity to impose a reasonable, cost-based fee for the provision of access to an individual's protected health information, upon request. Section 164.528 requires a covered entity to provide a requesting individual with an accounting of disclosures without

charge in any 12-month period but permits a covered entity to impose a reasonable, cost-based fee for each subsequent request for an accounting of disclosures during that 12-month period. Therefore, as a disclosure of protected health information under § 164.528 is similar to a disclosure under § 164.524 in that a covered entity may be paid a fee for making the disclosure, we have included disclosures pursuant to requests for accountings of disclosures in this exception. We note that this exception would not permit a covered entity to require that an individual pay a fee that is not otherwise permitted by §§ 164.524 or 164.528.

We propose an additional exception at § 164.508(a)(4)(ii)(G), pursuant to the authority granted to the Secretary in section 13405(d)(2)(G) of the HITECH Act to except from the authorization requirements at proposed § 164.508(a)(4)(i) disclosures that are required by law as permitted under § 164.512(a). Section 164.512(a) permits covered entities to use or disclose protected health information to the extent that such use or disclosure is required by law. We propose to add this exception to ensure that a covered entity can continue to disclose protected health information, where required by law, even if the covered entity receives remuneration for the disclosure. We request comment on the inclusion of such an exception.

Finally, we propose an additional exception at § 164.508(a)(4)(ii)(H), pursuant to the authority granted to the Secretary in section 13405(d)(2)(G), to except from the authorization requirements at proposed § 164.508(a)(4)(i) a disclosure of protected health information for any other purpose permitted by and in accordance with the applicable requirements of subpart E, as long as the only remuneration received by the covered entity is a reasonable, cost-based fee to cover the cost to prepare and transmit the protected health information for such purpose or is a fee otherwise expressly permitted by other law. We have included this proposed exception as necessary and appropriate to ensure that the proposed authorization requirement does not deter covered entities from disclosing protected health information for permissible purposes under subpart E just because they routinely receive payment equal to the cost of preparing, producing, or transmitting the protected health information. We emphasize that this exception would not apply if a covered entity received remuneration above the actual cost incurred to prepare, produce, or transmit the protected health information for the permitted purpose, unless such fee is expressly permitted by other law.

We recognize that many States have laws in place to limit the fees a health care provider can charge to prepare, copy, and transmit medical records. Some States simply require any reasonable costs incurred by the provider in making copies of the medical records to be paid for by the requesting party, while other States set forth specific cost limitations with respect to retrieval, labor, supplies, and copying costs and allow charges equal to actual mailing or shipping costs. Many of these State laws set different cost limitations based on the amount and type of information to be provided, taking into account whether the information is in paper or electronic form as well as whether the requested material includes x-rays, films, disks, tapes, or other diagnostic imaging. We intend that the reference in proposed § 164.508(a)(4)(ii)(H) to fees expressly permitted by other laws to include fees permitted by such State laws. Therefore, if a covered entity discloses protected health information in exchange for remuneration that conforms to an applicable State law with respect to such fees, the exception would apply and no authorization pursuant to § 164.508(a)(4)(i) would be required. We do note, however, that of the States that do have such laws in place, there is great variation regarding the types of document preparation activities for which a provider can charge as well as the permissible fee schedules for such preparation activities. We invite public comment on our proposal to include in § 164.508(a)(4)(ii)(H) a general exception for disclosures made for permissible purposes for which the covered entity received remuneration that was consistent with applicable State law.

We propose a conforming change to § 164.508(b)(1)(i) to include a reference to the authorization requirement in proposed § 164.508(a)(4)(i).

2. Research

a. Compound Authorizations

Section 164.508(b)(4) of the Privacy Rule prohibits covered entities from conditioning treatment, payment, enrollment in a health plan, or eligibility for benefits on the provision of an authorization. This limitation is intended to prevent covered entities from coercing individuals into signing an authorization for a use or disclosure that is not necessary to carry out the services that the covered entity provides to the individual. However, this section permits a covered entity to condition the provision of research-related treatment on obtaining the individual's authorization in limited situations, such as for a clinical trial. Permitting the use of protected health information is part of the decision to receive care through a clinical trial, and health care providers conducting such trials are able to condition research-related treatment on the individual's willingness to authorize the use or disclosure of protected health information for research associated with the trial.

Section 164.508(b)(3) generally prohibits what are termed "compound authorizations," *i.e.,* where an authorization for the use and disclosure of protected health information is combined with any other legal permission. However, § 164.508(b)(3)(i) carves out an exception to this general prohibition, permitting the combining of an authorization for a research study with any other written permission for the same study, including another authorization or consent to participate in the research. Nonetheless, § 164.508(b)(3)(iii) prohibits combining an authorization that conditions treatment, payment, enrollment in a health plan, or eligibility for benefits with an authorization for another purpose for which treatment, payment, enrollment, or eligibility may not be conditioned. This limitation on certain compound authorizations was intended to help ensure that individuals understand that they may decline the activity described in the unconditioned authorization yet still receive treatment or other benefits or services by agreeing to the conditioned authorization.

The impact of these authorization requirements and limitations can be seen during clinical trials that are associated with a corollary research activity, such as when protected health information is used or disclosed to create or to contribute to a central research database or repository. For example, § 164.508(b)(3)(iii) prevents covered entities from obtaining a single authorization for the use or disclosure of protected health information for a research study that includes both treatment as part of a clinical trial and tissue banking of specimens (and associated protected health information) collected, since a research-related treatment authorization generally is conditioned and a tissue banking authorization generally is not conditioned. Various groups, including researchers and professional organizations, have expressed concern at this lack of integration. The Secretary's Advisory Committee for Human Research Protections in 2004

(Recommendation V, in a letter to the Secretary of HHS, available at *http://www.hhs.gov/ohrp/sachrp/hipaalettertosecy090104.html*), as well as the Institute of Medicine (IOM) in its 2009 Report, "Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research" (Recommendation II.B.2), also made specific recommendations to allow combined authorizations for clinical trials and biospecimen storage. Research-related treatment offered through a clinical trial is nearly always conditioned upon signing the informed consent to participate in the trial and the authorization to use or disclose the individual's protected health information for the trial. Thus, covered entities must obtain separate authorizations from research participants for a clinical trial that also collects specimens with associated protected health information for a central repository. For clinical research trials that may have thousands of participants, documenting and storing twice as many authorizations is a major concern. There is also a concern that multiple forms may be confusing for research subjects. The Department has received reports that recruitment into clinical trials has been hampered, in part, because the multiplicity of forms for research studies dissuades individuals from participating in research. We have also heard that redundant information provided by two authorization forms (one for the clinical study and another for related research) diverts an individual's attention from other content that describes how and why the personal health information may be used.

While seeking Institutional Review Board (IRB) or Privacy Board waiver of the authorization requirement is an option under § 164.512 of the Privacy Rule, an IRB or Privacy Board is less likely to approve a request for a waiver of authorization for a foreseeable use or disclosure of protected health information to create and maintain or contribute to a central tissue or information repository if the covered entity is planning to seek informed consent from the individual for this purpose. Accordingly, the waiver provisions generally do not resolve concerns expressed by the research community.

We agree that allowing a covered provider to combine research authorizations would streamline the process for obtaining an individual's authorization for research and would make the documentation responsibilities of these covered entities more manageable. Such a modification would also result in an authorization that would be simpler and, therefore, more meaningful to the individual (in contrast to the individual receiving multiple forms that may be confusing). We, therefore, propose to amend § 164.508(b)(3)(i) and (iii) to allow a covered entity to combine conditioned and unconditioned authorizations for research, provided that the authorization clearly differentiates between the conditioned and unconditioned research components and clearly allows the individual the option to opt in to the unconditioned research activities. These provisions would allow covered entities to combine authorizations for scenarios that often occur in research studies. For example, a covered entity would be able to combine an authorization permitting the use and disclosure of protected health information associated with a specimen collection for a central repository and authorization permitting use and disclosure of protected health information for clinical research that conditions research-related treatment on the execution of a HIPAA authorization.

While the proposed modifications do not alter the core elements or required statements integral to a valid authorization, covered entities would have some flexibility with respect to how they met the authorization requirements. For example, covered entities could facilitate an individual's understanding of a compound authorization by describing the unconditioned research activity on a separate page of a compound authorization. They could also cross-reference relevant sections of a compound authorization to minimize the potential for redundant language. In addition, a covered entity could use a separate check-box for the unconditioned research activity to signify whether an individual has opted-in to the unconditioned research activity, while maintaining one signature line for the authorization. Alternatively, a covered entity could choose to provide a distinct signature line for the unconditioned authorization to signal that the individual is authorizing optional research that will not affect research-related treatment. We request comment on additional methods that would clearly differentiate to the individual the conditioned and unconditioned research activities on the compound authorization.

b. Authorizing Future Research Use or Disclosure

Research often involves obtaining health information and biological specimens to create a research database or repository for future research. For example, this frequently occurs where clinical trials are paired with corollary research activities, such as the creation of a research database or repository where information and specimens obtained from a research participant during the trial are transferred and maintained for future research. It also is our understanding that IRBs in some cases may approve an informed consent document for a clinical trial that also asks research participants to permit future research on their identifiable information or specimens obtained during the course of the trial, or may review an informed consent for a prior clinical trial to determine whether a subsequent research use is encompassed within the original consent.

The Department has interpreted the Privacy Rule, however, to require that authorizations for research be study specific for purposes of complying with the Rule's requirement at § 164.508(c)(1)(iv) that an authorization must include a description of each purpose of the requested use or disclosure. *See* 67 FR 53182, 53226, Aug. 14, 2002. In part, the Department's interpretation was based on a concern that patients could lack necessary information in the authorization to make an informed decision about the future research, due to a lack of information about the future research at the time the authorization was obtained. In addition, it was recognized that not all uses and disclosures of protected health information for a future research purpose would require a covered entity to re-contact the individual to obtain another authorization, to the extent other conditions in the Privacy Rule were met. For example, a covered entity could obtain a waiver of authorization from an IRB or Privacy Board as provided under § 164.512(i) or use or disclose only a limited data set pursuant to a data use agreement under § 164.514(e) for the future research purpose.

Subsequent to its issuing this interpretation, the Department has heard concerns from covered entities and researchers that the Department's interpretation encumbers secondary research, and limits an individual's ability to agree to the use or disclosure of their protected health information for future research without having to be re-contacted to sign multiple authorization forms at different points in the future. In addition, many commenters noted that the Department's interpretation limiting the scope of a HIPAA authorization for research appeared to diverge from the current practice under the Common Rule with respect to the

ability of a researcher to seek subjects' consent to future research so long as the future research uses are described in sufficient detail to allow an informed consent. These commenters, as well as the Secretary's Advisory Committee for Human Research Protections in 2004 (Recommendation IV, in a letter to the Secretary of HHS, available at *http://www.hhs.gov/ohrp/sachrp/hipaalettertosecy090104.html*) and the IOM in its 2009 Report entitled "Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research" (Recommendation II.B.1), have urged the Department to allow the HIPAA authorization to permit future research use and disclosure of protected health information or, at a minimum, for the Department to modify its interpretation to allow the authorization to encompass certain future use and disclosure of protected health information for research, provided certain parameters are met.

Given these concerns, in addition to the modifications mentioned in the prior section, the Department is considering whether to modify its interpretation that an authorization for the use or disclosure of protected health information for research be research-study specific. In particular, the Department is considering a number of options and issues in this area, including whether: (1) The Privacy Rule should permit an authorization for uses and disclosures of protected health information for future research purposes to the extent such purposes are adequately described in the authorization such that it would be reasonable for the individual to expect that his or her protected health information could be used or disclosed for such future research; (2) the Privacy Rule should permit an authorization for future research only to the extent the description of the future research included certain elements or statements specified by the Privacy Rule, and if so, what should those be; and (3) the Privacy Rule should permit option (1) as a general rule but require certain disclosure statements on the authorization in cases where the future research may encompass certain types of sensitive research activities, such as research involving genetic analyses or mental health research, that may alter an individual's willingness to participate in the research. We request comment on each of these options, including their impact on the conduct of research and patient understanding of authorizations.

We note that any modification in this area would not alter an individual's right to revoke the authorization for the use or disclosure of protected health information for future research at any time and that the authorization would have to include a description of how the individual may do so. We request comment on how a revocation would operate with respect to future downstream research studies.

The Department does not propose any specific modifications to the Privacy Rule at this time but requests public comment on the options identified above, as well as any others, for purposes of addressing this issue at the time the final rule is issued, if appropriate. In addition, any change in interpretation will be closely coordinated with the HHS Office for Human Research Protections (OHRP) and the FDA to ensure the Privacy Rule policies are appropriately harmonized with those under the HHS human subjects protections regulations (45 CFR part 46) and FDA human subjects protections regulations governing informed consent for research (21 CFR part 50).

E. Protected Health Information About Decedents

1. Section 164.502(f)—Period of Protection for Decedent Information

Section 164.502(f) requires covered entities to protect the privacy of a decedent's protected health information generally in the same manner and to the same extent that is required for the protected health information of living individuals. Thus, if an authorization is required for the use or disclosure of protected health information, a covered entity may use or disclose a decedent's protected health information in that situation only if the covered entity obtains an authorization from the decedent's personal representative. The personal representative for a decedent is the executor, administrator, or other person who has authority under applicable law to act on behalf of the decedent or the decedent's estate. The Department has heard a number of concerns since the publication of the Privacy Rule that it can be difficult to locate a personal representative to authorize the use or disclosure of the decedent's protected health information, particularly after an estate is closed. Furthermore, archivists, biographers and historians have expressed frustration regarding the lack of access to ancient or old records of historical value held by covered entities, even when there are likely few remaining individuals concerned with the privacy of such information. Archives and libraries may hold medical records that are centuries old. Furthermore, fragments of health information may be found throughout all types of archival holdings, such as correspondence files, diaries, and photograph collections, that are also in some cases centuries old. Currently, to the extent such information is maintained by a covered entity, it is subject to the Privacy Rule. For example, currently the Privacy Rule would apply in the same manner to the casebook of a 19th century physician as it would to the medical records of current patients of a physician.

Accordingly, we propose to amend § 164.502(f) to require a covered entity to comply with the requirements of the Privacy Rule with regard to the protected health information of a deceased individual for a period of 50 years following the date of death. We also propose to modify the definition of "protected health information" at § 160.103 to make clear that the individually identifiable health information of a person who has been deceased for more than 50 years is not protected health information under the Privacy Rule. We believe that fifty years is an appropriate time span, because by approximately covering the span of two generations we believe it will both protect the privacy interests of most, if not all, living relatives, or other affected individuals, and it reflects the difficulty of obtaining authorizations from personal representatives as time passes. A fifty-year period of protection also was suggested at a prior National Committee for Vital and Health Statistics (NCVHS) (the public advisory committee which advises the Secretary on the implementation of the Administrative Simplification provisions of HIPAA, among other issues) meeting, at which committee members heard testimony from archivists regarding the problems associated with applying the Privacy Rule to very old records. *See http://ncvhs.hhs.gov/050111mn.htm.* We request public comment on the appropriateness of this time period.

We note that these proposed modifications would have no impact on a covered entity's permitted disclosures related to decedents for law enforcement purposes (§ 164.512(f)(4)), to coroners or medical examiners and funeral directors (§ 164.512(g)), for research that is solely on the protected health information of decedents (§ 164.512(i)(1)(iii)), and for organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation (§ 164.512(h)).

These disclosures are governed by other provisions of the Privacy Rule.

2. Section 164.510(b)—Disclosures About a Decedent to Family Members and Others Involved in Care

Section 164.510(b) describes how a covered entity may use or disclose protected health information to persons, such as family members or others, who are involved in an individual's care or payment related to the individual's health care. We have received a number of questions about the scope of the section, specifically with regard to the protected health information of decedents. We have heard concerns that family members, relatives, and others, many of whom may have had access to the health information of the deceased individual prior to death, have had difficulty obtaining access to such information after the death of the individual, because many do not qualify as a "personal representative" under § 164.502(g)(4).

As such, we propose to amend § 164.510(b) to add a new paragraph (5), which would permit covered entities to disclose a decedent's information to family members and others who were involved in the care or payment for care of the decedent prior to death, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity. We propose to add conforming cross-references to paragraphs (b)(1)(i) and (ii) and (b)(4). We note that this disclosure would be permitted, but would not be required. We request comment on any unintended consequences that this permissive disclosure provision might cause.

We also note that these modifications do not change the authority of a decedent's personal representative with regard to the decedent's protected health information. Thus, a personal representative may continue to request access to or an accounting of a decedent's protected health information, and may continue to authorize uses and disclosures of the decedent's protected health information that are not otherwise permitted or required by the Privacy Rule.

F. Section 164.512(b)—Disclosure of Student Immunizations to Schools

The Privacy Rule, in § 164.512(b), recognizes that covered entities must balance protecting the privacy of health information with sharing health information with those responsible for ensuring public health and safety, and permits covered entities to disclose the minimum necessary protected health information to public health authorities or other designated persons or entities without an authorization for public health purposes specified by the Rule. Covered entities may disclose protected health information: (1) To a public health authority that is legally authorized to collect or receive the information for the purpose of preventing or controlling disease, injury, or disability (such as reporting communicable diseases, births, and deaths, or conducting public health interventions, investigations, and surveillance); (2) to a public health authority or other appropriate government authority to report child abuse if the authority is legally authorized to receive such reports; (3) to a person or entity subject to the jurisdiction of the FDA about the quality, safety, or effectiveness of an FDA-regulated product or activity for which the person or entity has responsibility (such as reporting adverse drug events to the drug manufacturer); (4) to notify a person that (s)he is at risk of contracting or spreading a disease or condition, as authorized by law, to carry out a public health intervention or investigation; and (5) to an employer under limited circumstances and conditions when the employer needs the information to comply with Occupational Safety and Health Administration (OSHA) or Mine Safety and Health Administration (MSHA) requirements. Any other disclosures that do not conform to these provisions, and that are not otherwise permitted by the Rule, require the individual's prior written authorization.

Schools play an important role in preventing the spread of communicable diseases among students by ensuring that students entering classes have been immunized. Most States have "school entry laws" which prohibit a child from attending school unless the school has proof that the child has been appropriately immunized. Typically, schools ensure compliance with those requirements by requesting the immunization records from parents (rather than directly from a health care provider), particularly because the Privacy Rule generally requires written authorization by the child's parent before a covered health care provider may disclose protected health information directly to the school. Some States allow a child to enter school provisionally for a period of 30 days while the school waits for the necessary immunization information.

We have heard concerns that the Privacy Rule may make it more difficult for parents to provide, and for schools to obtain, the necessary immunization documentation for students, which may prevent students' admittance to school. The NCVHS submitted these concerns to the HHS Secretary and recommended that HHS regard disclosure of immunization records to schools to be a public health disclosure. *See http://www.ncvhs.hhs.gov/040617l2.htm.*

As such, we propose to amend § 164.512(b)(1) by adding a new paragraph that permits covered entities to disclose proof of immunization to schools in States that have school entry or similar laws. While written authorization that complies with § 164.508 would no longer be required for disclosure of such information, the covered entity would still be required to obtain agreement, which may be oral, from a parent, guardian or other person acting *in loco parentis* for the individual, or from the individual him- or herself, if the individual is an adult or emancipated minor. Because the proposed provision would permit a provider to accept a parent's oral agreement to disclose immunization results to a school—as opposed to a written agreement—there is a potential for a miscommunication and later objection by the parent. We, therefore, request comment on whether the Privacy Rule should require that a provider document any oral agreement under this provision to help avoid such problems, or whether a requirement for written documentation would be overly cumbersome, on balance. We also request comment on whether the rule should mandate that the disclosures go to a particular school official and if so, who that should be.

In addition, the Privacy Rule does not currently define the term "school" and we understand that the types of schools subject to the school entry laws may vary by State. For example, depending on the State, such laws may apply to public and private elementary or primary schools and secondary schools (kindergarten through 12th grade), as well as daycare and preschool facilities, and post-secondary institutions. Thus, we request comment on the scope of the term "school" for the purposes of this section and whether we should include a specific definition of "school" within the regulation itself. In addition, we request comment on the extent to which schools that may not be subject to these school entry laws but that may also require proof of immunization have experienced problems that would warrant their being included in this category of public health disclosures.

Finally, we note that once a student's immunization records are obtained and maintained by an educational institution or agency to which the Family Educational Rights and Privacy

Act (FERPA) applies, the records are protected by FERPA, rather than the HIPAA Privacy Rule. *See* paragraphs (2)(i) and (2)(ii) of the definition of "protected health information" at § 160.103, which exclude from coverage under the Privacy Rule student records protected by FERPA. In addition, for more information on the intersection of FERPA and HIPAA, readers are encouraged to consult the Joint HHS/ED Guidance on the Application of FERPA and HIPAA to Student Health Records, available at *http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hipaaferpajointguide.pdf.*

G. Section 164.514(d)—Minimum Necessary

Section 164.502(b)(1) of the Privacy Rule requires covered entities to limit uses and disclosures of, and requests for, protected health information to "the minimum necessary to accomplish the intended purpose of the use, disclosure, or request." Section 164.502(b)(2) outlines situations in which the minimum necessary rule does not apply. With respect to uses of protected health information, § 164.514(d)(2) requires covered entities to identify workforce members who need access to protected health information, to identify the categories and conditions of such access, and to make reasonable efforts to limit access consistent with such policies. With respect to disclosures of, and requests for, protected health information, § 164.514(d)(3) and (4) require that covered entities adopt policies and procedures addressing minimum necessary, including with regard to uses and disclosures that occur routinely.

Section 13405(b)(1)(A) of the HITECH Act provides that a covered entity shall be treated as being in compliance with the minimum necessary requirements with respect to the use or disclosure of or the request for protected health information "only if the covered entity limits such protected health information, to the extent practicable, to the limited data set (as defined in section 164.514(e)(2) of such title) or, if needed by such entity, to the minimum necessary." Section 13405(b)(1)(B) requires the Secretary to issue guidance on what constitutes "minimum necessary" within 18 months after the date of enactment. This guidance must take into account the guidance required by section 13424(c), relating to the de-identification of protected health information, as well as "the information necessary to improve patient outcomes and to detect, prevent, and manage chronic disease." Section 13405(b)(1)(C) provides that the provisions of paragraph (A) no longer apply as of the effective date of the guidance issued under paragraph (B).

Section 13405(b)(2) provides that, with respect to disclosures of protected health information, the covered entity or business associate making the disclosure shall determine what constitutes the minimum necessary. Section 13405(b)(3) provides that section 13405(b)(1) does not affect the application of the exceptions to the minimum necessary requirement, while section 13405(b)(4) provides that nothing in subsection (b) is to be construed as affecting the use or disclosure of or request for de-identified health information.

Section 13405(b)(1)(A) requires that covered entities consider the feasibility of utilizing the limited data set in complying with the minimum necessary requirements of the Privacy Rule. However, that provision also permits a covered entity to employ its traditional minimum necessary policies and procedures if it decides that the limited data set will not meet the needs of the particular use, disclosure, or request in question. The requirement of this section, moreover, is an interim one; under section 13405(b)(1)(C), issuance of the guidance required by section 13405(b)(1)(B) effectively sunsets the requirement of section 13405(b)(1)(A).

For purposes of the required guidance, we take this opportunity to solicit public comment on what aspects of the minimum necessary standard covered entities and business associates believe would be most helpful to have the Department address in the guidance and the types of questions entities may have about how to appropriately determine the minimum necessary for purposes of complying with the Privacy Rule. We propose to leave the current regulatory text unchanged in this rulemaking as the issuance of the required guidance will obviate the need to make any regulatory modifications in this area.

H. Section 164.514(f)—Fundraising

Section 164.514(f)(1) of the Privacy Rule permits a covered entity to use, or disclose to a business associate or an institutionally related foundation, the following protected health information for its own fundraising purposes without an individual's authorization: (1) Demographic information relating to an individual; and (2) the dates of health care provided to an individual. Section 164.514(f)(2) of the Privacy Rule requires a covered entity that plans to use or disclose protected health information for fundraising under this paragraph to inform individuals in its notice of privacy practices that it may contact them to raise funds for the covered entity. In addition, § 164.514(f)(2) requires that a covered entity include in any fundraising materials it sends to an individual a description of how the individual may opt out of receiving future fundraising communications and that a covered entity must make reasonable efforts to ensure that individuals who do opt out are not sent future fundraising communications.

Section 13406(b) of the HITECH Act, which became effective on February 18, 2010, requires the Secretary to provide by rule that a covered entity provide the recipient of any fundraising communication with a clear and conspicuous opportunity to opt out of receiving any further fundraising communications. Additionally, section 13406(b) states that if an individual does opt out of receiving further fundraising communications, the individual's choice to opt out must be treated as a revocation of authorization under § 164.508 of the Privacy Rule.

We propose a number of changes to the Privacy Rule's fundraising requirements to implement these statutory provisions. First, we propose to strengthen the opt out by requiring that a covered entity provide, with each fundraising communication sent to an individual under these provisions, a clear and conspicuous opportunity for the individual to elect not to receive further fundraising communications. To satisfy this requirement, we also propose to require that the method for an individual to elect not to receive further fundraising communications may not cause the individual to incur an undue burden or more than nominal cost. We encourage covered entities to consider the use of a toll-free phone number, an e-mail address, or similar opt out mechanism that would provide individuals with a simple, quick, and inexpensive way to opt out of receiving future communications. We note that we would consider requiring individuals to write and send a letter to the covered entity asking not to receive future fundraising communications to constitute an undue burden on the individual for purposes of this proposed requirement.

We also propose to provide that a covered entity may not condition treatment or payment on an individual's choice with respect to receiving fundraising communications. We believe this modification would implement the language in section 13406(b) of the HITECH Act that provides that an election by an

individual not to receive further fundraising communications shall be treated as a revocation of authorization under the Privacy Rule. The legislative history of the HITECH Act indicates that it was Congress' intent with this language that the protections that apply under § 164.508 to an individual who has revoked an authorization similarly apply to an individual who has opted out of fundraising communications, "including the right not to be denied treatment as a result of making that choice." *See* H.R. Conf. Rep. 111–16, p. 498. Therefore, we make clear in this proposed rule that a covered entity would not be permitted to condition treatment or payment for care on an individual's choice of whether to receive fundraising communications.

Further, we propose to provide that a covered entity may not send fundraising communications to an individual who has elected not to receive such communications. This proposed language would strengthen the current requirement at § 164.514(f)(2)(iii) that a covered entity make "reasonable efforts" to ensure that those individuals who have opted out of receiving fundraising communications are not sent such communications. We have proposed stronger language to make clear the expectation that covered entities abide by an individual's decision not to receive fundraising communications, as well as to make the fundraising opt out operate more like a revocation of authorization, consistent with the statutory language and legislative history of section 13406(b) of the HITECH Act discussed above.

With respect to the operation of the opt out, we request comment regarding to what fundraising communications the opt out should apply. For example, if an individual receives a fundraising letter and opts out of receiving future fundraising communications, should the opt out apply to all future fundraising communications or should and can the opt out be structured in a way to only apply to the particular fundraising campaign described in the letter? In addition, given that we would require the opt out method to be simple and quick for the individual to exercise, such as the use of a phone number or e-mail address, we request comment on whether the Rule should allow a similar method, short of the individual signing an authorization, by which an individual who has previously opted out can put his or her name back on an institution's fundraising list.

We propose to retain the requirement that a covered entity that intends to contact the individual to raise funds under these provisions must include a statement to that effect in its notice of privacy practices. However, we do propose to modify the required statement slightly, as indicated below in the discussion of the notice requirements at § 164.520, by requiring that the notice also inform individuals that they have a right to opt out of receiving such communications. We also propose to move all of the fundraising requirements described above to § 164.514(f)(1), given that the proposed provisions for subsidized treatment communications discussed above now would be located at § 164.514(f)(2).

In addition to the above modifications proposed in response to the HITECH Act, we also solicit public comment on the requirement at § 164.514(f)(1) which limits the information a covered entity may use or disclose for fundraising demographic information about and dates of health care service provided to an individual. Since the promulgation of the Privacy Rule, certain covered entities have raised concerns regarding this limitation, maintaining that the Privacy Rule's prohibition on the use or disclosure of certain treatment information without an authorization, such as the department of service where care was received and outcomes information, harms their ability to raise funds from often willing and grateful patients. In particular, covered entities have argued that the restrictions in the Privacy Rule prevent them from targeting their fundraising efforts and avoiding inappropriate solicitations to individuals who may have had a bad treatment outcome, and obtaining an individual's authorization for fundraising as the individual enters or leaves the hospital for treatment is often impracticable or inappropriate. NCVHS also held a hearing and heard public testimony on this issue in July 2004. After considering the testimony provided, the NCVHS recommended to the Secretary that the Privacy Rule should allow covered entities to use or disclose information related to the patient's department of service (broad designations, such as surgery or oncology, but not narrower designations or information relating to diagnosis or treating physician) for fundraising activities without patient authorization. NCVHS also recommended that a covered entity's notice of privacy practices inform patients that their department of service information may be used in fundraising, and that patients should be afforded the opportunity to opt out of the use of their department of service information for fundraising or all fundraising contacts altogether. *See http://www.ncvhs.hhs.gov/040902lt1.htm.*

In light of these concerns and the prior recommendation of the NCVHS, the Department takes this opportunity to solicit public comment on whether and how the current restriction on what information may be used and disclosed should be modified to allow covered entities to more effectively target fundraising and avoid inappropriate solicitations to individuals, as well as to reduce the need to send solicitations to all patients. In particular, we solicit comment on: (1) Whether the Privacy Rule should allow additional categories of protected health information to be used or disclosed for fundraising, such as department of service or similar information, and if so, what those categories should be; (2) the adequacy of the minimum necessary standard to appropriately limit the amount of protected health information that may be used or disclosed for fundraising purposes; or (3) whether the current limitation should remain unchanged. We also solicit comment on whether, if additional information is permitted to be used or disclosed for fundraising absent an authorization, covered entities should be required to provide individuals with an opportunity to opt out of receiving any fundraising communications before making the first fundraising solicitation, in addition to the opportunity to opt out with every subsequent communication. We invite public comment on whether such a pre-solicitation opt out would be workable for covered entities and individuals and what mechanisms could be put into place to implement the requirement.

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

Section 164.520 of the Privacy Rule sets out the requirements for most covered entities to have and to distribute a notice of privacy practices (NPP). The NPP must describe the uses and disclosures of protected health information a covered entity is permitted to make, the covered entity's legal duties and privacy practices with respect to protect protected health information, and the individual's rights concerning protected health information.

With regard to the description of permitted uses and disclosures, § 164.520(b)(1)(ii) requires a covered entity to include separate statements about the uses and disclosures that the covered entity intends to make for certain treatment, payment, or health care operations activities. Further, § 164.520(b)(1)(ii)(E) currently requires

that the NPP contain a statement that any uses and disclosures other than those permitted by the Privacy Rule will be made only with the written authorization of the individual, and that the individual has the right to revoke an authorization pursuant to § 164.508(b)(5). The purpose of this statement is to put individuals on notice that covered entities may make certain uses and disclosures only with an authorization from the individual.

Section 164.520(b)(1)(iv) requires that the NPP contain statements regarding the rights of individuals with respect to their protected health information and a brief description of how individuals may exercise such rights. Section 164.520(b)(1)(iv)(A) currently requires a statement and a brief description addressing an individual's right to request restrictions on the uses and disclosures of protected health information pursuant to § 164.522(a), including the fact that the covered entity is not required to agree to this request.

We propose to amend § 164.520(b)(1)(ii)(E) to require that the NPP include a statement that describes the uses and disclosures of protected health information that require an authorization under § 164.508(a)(2) through (a)(4), and to provide that other uses and disclosures not described in the notice will be made only with the individual's authorization. The proposed provision would ensure that covered entities provide notice to individuals indicating that most disclosures of protected health information for which the covered entity receives remuneration would require the authorization of the individual. Such uses and disclosures may have previously been permitted under other provisions of the Rule but now require authorization, as discussed in connection with proposed § 164.508(a)(4).

We propose to require, in addition, that covered entities provide notice that most uses and disclosures of psychotherapy notes and for marketing purposes require an authorization so that individuals will be made aware of all situations in which authorization is required. We are concerned that omission of such a specific statement may be somewhat misleading or confusing, in that the NPP would state that the covered entity may use or disclose protected health information without authorization for purposes of treatment, payment, and health care operations and some individuals might assume that psychotherapy notes and marketing would be covered by these permissions.

Section 164.520(b)(1)(iii) requires a covered entity to include in its NPP separate statements about certain activities if the covered entity intends to engage in any of the activities. In particular, § 164.520(b)(1)(iii) requires a separate statement in the notice if the covered entity intends to contact the individual to provide appointment reminders or information about treatment alternatives or other health-related benefits or services; to contact the individual to fundraise for the covered entity; or, with respect to a group health plan, to disclose protected health information to the plan sponsor.

We propose the following changes to these provisions. First, we propose to modify § 164.520(b)(1)(iii)(A) to align the required statement with the proposed modifications related to marketing and subsidized treatment communications. A covered health care provider that intends to send treatment communications to the individual in accordance with proposed § 164.514(f)(2) concerning treatment alternatives or other health-related products or services where the provider receives financial remuneration in exchange for making the communication would be required to inform the individual in advance in the NPP, as well as inform the individual that he or she has the opportunity to opt out of receiving such communications. Second, at § 164.520(b)(1)(iii)(B) we propose to require that if a covered entity intends to contact the individual to raise funds for the entity as permitted under § 164.514(f)(1), the covered entity must not only inform the individual in the NPP of this intention but also that the individual has the right to opt out of receiving such communications.

We also propose to modify the requirement of § 164.520(b)(1)(iv)(A) which requires covered entities to notify individuals of the individuals' right to request restrictions. This provision currently includes a requirement that the NPP state that the covered entity is not required to agree to such a request. Since this statement will no longer be accurate when the modifications to proposed § 164.522(a)(1)(vi) that are required by the HITECH Act are made (*see* discussion in the following section), proposed § 160.520(b)(1)(iv)(A) would require, in addition, that the statement include an exception for requests under § 164.522(a)(1)(vi).

Under subpart D of part 164, covered entities now have new obligations to comply with the requirements for notification to affected individuals, the media, and the Secretary following a breach of unsecured protected health information. We request comment on whether the Privacy Rule should require a specific statement regarding this new legal duty and what particular aspects of this new duty would be important for individuals to be notified of in the NPP.

The proposed modifications to § 164.520 represent material changes to the NPP of covered entities. Section 164.520(b)(3) requires that when there is a material change to the NPP, covered entities must promptly revise and distribute the NPP as outlined by § 164.520(c). Section 164.520(c)(1)(i)(C) requires that health plans provide notice to individuals covered by the plan within 60 days of any material revision to the NPP. We recognize that revising and redistributing a NPP may be costly for health plans and request comment on ways to inform individuals of this change to privacy practices without unduly burdening health plans. In particular, we are considering a number of options in this area: (1) Replace the 60-day requirement with a requirement for health plans to revise their NPPs and redistribute them (or at least notify members of the material change to the NPP and how to obtain the revised NPP) in their next annual mailing to members after a material revision to the NPP, such as at the beginning of the plan year or during the open enrollment period; (2) provide a specified delay or extension of the 60-day timeframe for health plans; (3) retain the provision generally to require health plans to provide notice within 60-days of a material revision but provide that the Secretary will waive the 60-day timeframe in cases where the timing or substance of modifications to the Privacy Rule call for such a waiver; or (4) make no change, and thus, require that health plans provide notice to individuals within 60 days of the material change to the NPP that would be required by this proposed rule. We request comment on these options, as well as on any other options for informing individuals in a timely manner of this proposed or other material changes to the NPP.

Section 164.520(c)(2)(iv) requires that when a health care provider with a direct treatment relationship with an individual revises the NPP, the health care provider must make the NPP available upon request on or after the effective date of the revision and must comply with the requirements of § 164.520(c)(2)(iii) to have the NPP available at the delivery site and to post the notice in a clear and prominent location. We do not believe these requirements will be overly burdensome on health care providers and do not propose changes to them, but we request comment on this issue.

J. Section 164.522(a)—Right To Request Restriction of Uses and Disclosures

Section 164.522(a) of the Privacy Rule requires covered entities to permit individuals to request that a covered entity restrict uses or disclosures of their protected health information for treatment, payment, and health care operations purposes, as well as for disclosures to family members and certain others permitted under § 164.510(b). While covered entities are not required to agree to such requests for restrictions, if a covered entity does agree to restrict the use or disclosure of an individual's protected health information, the covered entity must abide by that restriction, except in emergency circumstances when the information is required for the treatment of the individual. Section 164.522 also includes provisions for the termination of such a restriction and requires that covered entities that have agreed to a restriction document the restriction in writing.

Section 13405(a) of the HITECH Act, which became effective February 18, 2010, requires that when an individual requests a restriction on disclosure pursuant to § 164.522, the covered entity agree to the requested restriction unless otherwise required by law, if the request for restriction is on disclosures of protected health information to a health plan for the purpose of carrying out payment or health care operations and if the restriction applies to protected health information that pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full. This statutory requirement overrides the provision in § 164.522(a)(1)(ii) that the covered entity is not required to agree to requests for restrictions and requires that we modify the regulation.

To implement section 13405(a), we propose to add a new § 164.522(a)(1)(vi) to describe the elements of the required restriction. We also propose to add conforming language to § 164.522(a)(1)(ii) to reflect the mandatory nature of the restriction as required by the statute. Finally, we propose conforming modifications to § 164.522(a)(2) and (3), which address terminating and documentation of restrictions. We discuss these modifications in more detail below.

We propose to add a new paragraph (vi) to § 164.522(a)(1), which would require a covered entity, upon request from an individual, to agree to a restriction on the disclosure of protected health information to a health plan if: (A) the disclosure is for the purposes of carrying out payment or healthcare operations and is not otherwise required by law; and (B) the protected health information pertains solely to a health care item or service for which the individual, or person on behalf of the individual other than the health plan, has paid the covered entity in full. We also propose to modify the language in § 164.522(a)(1)(ii), which states that a covered entity is not required to agree to a restriction, to refer to this exception to that general rule. We note that under the Privacy Rule, a covered entity may make a disclosure to a business associate of another covered entity only where the disclosure would be permitted directly to the other covered entity. Thus, in cases where an individual has exercised his or her right to have a restriction placed under this paragraph on a disclosure to a health plan, the covered entity is also prohibited from making such disclosure to a business associate of the health plan.

Section 13405(a) makes clear that an individual has a right to have disclosures regarding certain health care items or services for which the individual pays out of pocket in full restricted from a health plan. We believe the Act provides the individual with the right to determine for which health care items or services the individual wishes to pay out of pocket and restrict. Thus, we do not believe a covered entity could require individuals who wish to restrict disclosures about only certain health care items or services to a health plan to restrict disclosures of protected health information regarding all health care to the health plan—*i.e.,* to require an individual to have to pay out of pocket for all services to take advantage of this right regardless of the particular health care item or service about which the individual requested the restriction. We believe such a policy would be contrary to Congressional intent, in that it would discourage individuals from requesting restrictions in situations where Congress clearly intended they be able to do so. For example, an individual who regularly visits the same provider for the treatment of both asthma and diabetes must be able to request, and have the provider honor, a restriction on the disclosure of diabetes-related treatment to the health plan as long as the individual pays out of pocket for this care. The provider cannot require that the individual apply the restriction to all care given by the provider and, as a result, cannot require the individual to pay out of pocket for both the diabetes and asthma-related care in order to have the restriction on the diabetes care honored. We encourage covered entities to work with individuals who wish to restrict certain information from disclosure to health plans to determine the best method for ensuring that the appropriate information is restricted from disclosure to a health plan.

Due to the myriad of treatment interactions between covered entities and individuals, we recognize that this provision may be more difficult to implement in some circumstances than in others, and we request comment on the types of interactions between individuals and covered entities that would make requesting or implementing a restriction more difficult. For example, an individual visits a provider for treatment of a condition, and the individual requests the provider not disclose information about the condition to the health plan and pays out of pocket for the care. The provider prescribes a medication to treat the condition, and the individual also wishes to restrict the health plan from receiving information about the medication. Many providers electronically send prescriptions to the pharmacy to be filled so that the medication is ready when the individual arrives to pick it up; however, at the point the individual arrives at the pharmacy, the pharmacy would have already sent the information to the health plan for payment, not permitting the individual an opportunity to request a restriction at the pharmacy. A provider who knows that an individual intends to request such a restriction can always provide the individual with a paper prescription to take to the pharmacy, allowing the individual an opportunity to request that the pharmacy restrict the disclosure of information relating to the medication. However, this might not be practical in every case, especially as covered entities begin to replace paper-based systems with electronic systems. We request comment on this issue, and we ask specifically for suggestions of methods through which a provider, using an automated electronic prescribing tool, could alert the pharmacy that the individual may wish to request that a restriction be placed on the disclosure of their information to the health plan and that the individual intends to pay out of pocket for the prescription.

Additionally, we request comment on the obligation of covered health care providers that know of a restriction to inform other health care providers downstream of such restriction. For example, a provider has been treating an individual for an infection for several

months pursuant to the individual's requested restriction that none of the protected health information relating to the treatment of the infection be disclosed to the individual's health plan. If the individual requests that the provider send a copy of his medical records to another health care provider for treatment, what, if any, obligation should the original provider have to notify the recipient provider (including a pharmacy filling the individual's prescription) that the individual has placed a restriction upon much of the protected health information in the medical record? We request comment on whether a restriction placed upon certain protected health information should apply to, and the feasibility of it continuing to attach to, such information as it moves downstream, or if the restriction should no longer apply until the individual visits the new provider for treatment or services, requests a restriction, and pays out of pocket for the treatment. In addition, we request comment on the extent to which technical capabilities exist that would facilitate notification among providers of restrictions on the disclosure of protected health information, how widely these technologies are currently utilized, and any limitations in the technology that would require additional manual or other procedures to provide notification of restrictions.

In accordance with the HITECH Act, proposed § 164.522(a)(1)(vi)(A) would permit a covered entity to disclose protected health information to a health plan if such disclosure is required by law, despite an individual's request for a restriction. We note that the term "required by law" is defined at § 164.103. We request comment on examples of types of disclosures that may fall under this provision.

With respect to the proposed requirement in § 164.522(a)(1)(vi)(B) that the covered entity be paid in full for the health care item or service for which the individual requests a restriction, we have added some language to the statutory provision to ensure that this requirement not be limited to solely the individual as the person paying the covered entity for the individual's care. There are many situations in which family members or other persons may pay for the individual's treatment. Thus, this proposed paragraph would provide that as long as the covered entity is paid for the services by the individual or another person on behalf of the individual other than the health plan, the covered entity would be required to abide by the restriction.

With regard to proposed § 164.522(a)(1)(vi)(B), we emphasize that when an individual requests a restriction of information to a health plan and pays out of pocket for the treatment or service, the individual should not expect that this payment will count towards the individual's out of pocket threshold with respect to his or her health plan benefits. As the very nature of this provision is to restrict information from flowing to the health plan, the health plan will be unaware of any payment for treatment or services for which the individual has requested a restriction, and thus, this out of pocket payment cannot be used to reach the threshold for benefits a health plan offers.

We request public comment on how this provision will function with respect to HMOs. A provider who contracts with an HMO generally receives a fixed payment from an HMO based on the number of patients seen and not based on the treatment or service provided, and an individual patient of that provider pays a flat co-payment for every visit regardless of the treatment or service received. Therefore, it is our understanding that under most current HMO contracts with providers an individual could not pay the provider for the treatment or service received. Thus, individuals who belong to an HMO may have to use an out-of-network provider if they wish to ensure that certain protected health information is not disclosed to the HMO. We request public comment on this issue.

Finally, with respect to proposed § 164.522(a)(1)(vi)(B), we emphasize that if an individual's out of pocket payment for a health care item or service to restrict disclosure of the information to a health plan is not honored (for example, the individual's check bounces), the covered entity may then submit the information to the health plan for payment as the individual has not fulfilled the requirements necessary to obtain a restriction. We do not believe that the statutory intent was to permit individuals to avoid payment to providers for the health care services they provide. Therefore, if an individual does not pay in full for the treatment or services provided to the individual, then the provider is under no obligation to restrict the information and may disclose the protected health information to the health plan to receive payment. However, we expect covered entities to make some attempt to resolve the payment issue with the individual prior to sending the protected health information to the health plan, such as by notifying the individual that his or her payment did not go through and to give the individual an opportunity to submit payment. We request comment on the extent to which covered entities must make reasonable efforts to secure payment from the individual prior to submitting protected health information to the health plan for payment.

We propose to modify § 164.522(a)(2) and (3) regarding terminating restrictions and documentation of restrictions to reflect the addition of these new requirements. First, we would modify the language in § 164.522(a)(2) to remove the term "its agreement to" to clarify that the termination provisions apply to all restrictions, even those which are mandatory for the covered entity. Similarly, we would modify the language in § 164.522(a)(3) regarding documentation to remove the words "that agrees to a restriction" to make clear that the documentation requirements apply to all restrictions, including those that would be required by proposed paragraph (a)(1)(vi).

Additionally, we propose to modify § 164.522(a)(2)(iii) to conform to proposed paragraph (a)(1)(vi), requiring the mandatory restrictions for certain disclosures to health plans. In particular, in cases in which a covered entity is required to agree to a restriction under this section, we propose to add a new paragraph (A) to paragraph (a)(2)(iii) to clarify that a covered entity may not unilaterally terminate such a restriction.

The proposed modifications would operate as follows with respect to termination of a restriction under proposed paragraph (a)(1)(vi). For example, an individual who has requested a restriction on the disclosure of protected health information to a health plan about a particular health care service visits the provider for follow-up treatment, asks the provider to bill the health plan for the follow-up visit, and does not request a restriction at the time, nor pays out of pocket for the follow-up treatment. In such circumstances, there is no restriction in effect with respect to the follow-up treatment. However, the provider may need to submit information about the original treatment to the health plan so that it can determine the medical appropriateness or medical necessity of the follow-up care provided to the individual. At this time, we would consider the lack of a restriction with respect to the follow-up treatment to extend to any protected health information necessary to effect payment for such treatment, even if such information pertained to prior treatment that was subject to a restriction. We encourage covered entities to have an open dialogue with individuals to

ensure that they are aware that protected health information may be disclosed to the health plan unless they request an additional restriction and pay out of pocket for the follow-up care. We request public comment on this issue.

K. Section 164.524—Access of Individuals to Protected Health Information

Section 164.524 of the Privacy Rule currently establishes, with limited exceptions, an enforceable means by which individuals have a right to review or obtain copies of their protected health information, to the extent such information is maintained in the designated record set(s) of a covered entity. An individual's right of access exists regardless of the format of the protected health information, and the standards and implementation specifications that address individuals' requests for access and timely action by the covered entity (*i.e.,* provision of access, denial of access, and documentation) apply to an electronic environment in a similar manner as they do to a paper-based environment. *See The HIPAA Privacy Rule's Right of Access and Health Information Technology* (providing guidance with respect to how § 164.524 applies in an electronic environment and how health information technology can facilitate providing individuals with this important privacy right), available at: *http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/eaccess.pdf*.

Section 13405(e) of the HITECH Act, which became effective February 18, 2010, strengthens the Privacy Rule's right of access with respect to covered entities that use or maintain an electronic health record on an individual. Section 13405(e) provides that when a covered entity uses or maintains an electronic health record with respect to protected health information of an individual, the individual shall have a right to obtain from the covered entity a copy of such information in an electronic format and the individual may direct the covered entity to transmit such copy directly to the individual's designee, provided that any such choice is clear, conspicuous, and specific. Section 13405(e) also provides that any fee imposed by the covered entity for providing such an electronic copy shall not be greater than the entity's labor costs in responding to the request for the copy.

Section 13405(e) applies by its terms only to protected health information in electronic health records. However, incorporating these new provisions in such a limited manner in the Privacy Rule could result in a complex set of disparate requirements for access to protected health information in electronic health records systems versus other types of electronic records systems. As such, the Department proposes to use its authority under section 264(c) of HIPAA to prescribe the rights individuals should have with respect to their individually identifiable health information to strengthen the right of access as provided under section 13405(e) of the HITECH Act more uniformly to all protected health information maintained in one or more designated record sets electronically, regardless of whether the designated record set is an electronic health record. We discuss our proposed amendments to each provision implicated by section 13405(e) more specifically below.

Section 164.524(c)(2) of the Privacy Rule requires a covered entity to provide the individual with access to the protected health information in the form or format requested by the individual, if it is readily producible in such form or format, or, if not, in a readable hard copy form or such other form or format as agreed to by the covered entity and the individual. Section 13405(e) of the HITECH Act expands this requirement by explicitly requiring a covered entity that uses or maintains an electronic health record with respect to protected health information to provide the individual with a copy of such information in an electronic format.

We propose to implement this statutory provision, in conjunction with our broader authority under section 264(c) of HIPAA, by requiring, in proposed § 164.524(c)(2)(ii), that if the protected health information requested is maintained electronically in one or more designated record sets, the covered entity must provide the individual with access to the electronic information in the electronic form and format requested by the individual, if it is readily producible, or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual. This provision would require any covered entity that electronically maintains the protected health information about an individual, in one or more designated record sets, to provide the individual with an electronic copy of such information (or summary or explanation if agreed to by the individual in accordance with proposed § 164.524(c)(2)(iii)) in the electronic form and format requested or in an otherwise agreed upon form and format. While an individual's right of access to an electronic copy of protected health information is currently limited under the Privacy Rule by whether the form or format requested is readily producible, covered entities that maintain such information electronically in a designated record set would be required under these proposed modifications to provide some type of electronic copy, if requested by an individual.

Because we do not want to bind covered entities to standards that may not yet be technologically mature, we propose to permit covered entities to make some other agreement with individuals as to an alternative means by which they may provide a readable electronic copy, to the extent the requested means is not readily producible. If, for example, a covered entity received a request to provide electronic access via a secure Web-based portal, but the only readily producible version of the protected health information was in portable document format (PDF), proposed § 164.524(c)(2)(ii) would require the covered entity to provide the individual with a PDF copy of the protected health information, if agreed to by the covered entity and the individual. We note that while there may be circumstances where a covered entity determines that it can comply with the Privacy Rule's right of access by providing individuals with limited access rights to their electronic health record, such as through a secure Web-based portal, nothing under the current Rule or proposed modifications would require a covered entity to do so where the covered entity determines it is not reasonable or appropriate.

We note that the option of arriving at an alternative agreement that satisfies both parties is already part of the requirement to provide access under § 164.524(c)(2)(i), so extension of such a requirement to electronic access should present few implementation difficulties. Further, as with other disclosures of protected health information, in providing the individual with an electronic copy of protected health information through a Web-based portal, e-mail, on portable electronic media, or other means, covered entities should ensure that reasonable safeguards are in place to protect the information. We also note that the proposed modification presumes that covered entities have the capability of providing an electronic copy of protected health information maintained in their designated record set(s) electronically through a secure Web-based portal, via e-mail, on portable electronic media, or other manner. We invite public comment on this presumption.

Section 164.524(c)(3) of the Privacy Rule currently requires the covered entity to provide the access requested by the individual in a timely manner, which includes arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy of protected health information at the individual's request. The Department has previously interpreted this provision as requiring a covered entity to mail the copy of protected health information to an alternative address requested by the individual, provided the request was clearly made by the individual and not a third party. Section 13405(e)(1) of the HITECH Act provides that if the individual chooses, he or she shall have a right to direct the covered entity to transmit an electronic copy of protected health information in an electronic health record directly to an entity or person designated by the individual, provided that such choice is clear, conspicuous, and specific.

Based on section 13405(e)(1) of the HITECH Act and our authority under section 264(c) of HIPAA, we propose to expand § 164.524(c)(3) to expressly provide that, if requested by an individual, a covered entity must transmit the copy of protected health information directly to another person designated by the individual. This proposed amendment is consistent with the Department's prior interpretation on this issue and would apply without regard to whether the protected health information is in electronic or paper form. We propose to implement the requirement of section 13405(e)(1) that the individual's "choice [be] clear, conspicuous, and specific" by requiring that the individual's request be "in writing, signed by the individual, and clearly identify the designated person and where to send the copy of protected health information." We note that the Privacy Rule allows for electronic documents to qualify as written documents for purposes of meeting the Rule's requirements, as well as electronic signatures to satisfy any requirements for a signature, to the extent the signature is valid under applicable law. Thus, a covered entity could employ an electronic process for receiving an individual's request to transmit a copy of protected health information to his or her designee under this proposed provision. Whether the process is electronic or paper-based, a covered entity must implement reasonable policies and procedures under § 164.514(h) to verify the identity of any person who requests protected health information, as well as implement reasonable safeguards under § 164.530(c) to protect the information that is used or disclosed.

Section 164.524(c)(4) of the Privacy Rule currently permits a covered entity to impose a reasonable, cost-based fee for a copy of protected health information (or a summary or explanation of such information). However, such a fee may only include the cost of: (1) The supplies for, and labor of, copying the protected health information; (2) the postage associated with mailing the protected health information, if applicable; and (3) the preparation of an explanation or summary of the protected health information, if agreed to by the individual. With respect to providing a copy (or summary or explanation) of protected health information from an electronic health record in electronic form, however, section 13405(e)(2) of the HITECH Act provides that a covered entity may not charge more than its labor costs in responding to the request for the copy.

In response to section 13405(e)(2) of the HITECH Act, we propose to amend § 164.524(c)(4)(i) to identify separately the labor for copying protected health information, whether in paper or electronic form, as one factor that may be included in a reasonable cost-based fee. While we do not propose more detailed considerations for this factor within the regulatory text, we retain all prior interpretations of labor with respect to paper copies—that is, that the labor cost of copying may not include the costs associated with searching for and retrieving the requested information. With respect to electronic copies, we believe that a reasonable cost-based fee includes costs attributable to the labor involved to review the access request and to produce the electronic copy, which we expect would be negligible. However, we would not consider a reasonable cost-based fee to include a standard "retrieval fee" that does not reflect the actual labor costs associated with the retrieval of the electronic information or that reflects charges that are unrelated to the individual's request (*e.g.,* the additional labor resulting from technical problems or a workforce member's lack of adequate training). We invite public comment on this aspect of our rulemaking, specifically with respect to what types of activities related to managing electronic access requests should be compensable aspects of labor.

We also propose to amend § 164.524(c)(4)(ii) to provide separately for the cost of supplies for creating the paper copy or electronic media (*i.e.,* physical media such as a compact disc (CD) or universal serial bus (USB) flash drive), if the individual requests that the electronic copy be provided on portable media. This reorganization and the addition of the phrase "electronic media" reflects our understanding that since section 13405(e)(2) of the HITECH Act permits only the inclusion of labor costs in the charge for electronic copies, it by implication excludes charging for the supplies that are used to create an electronic copy of the individual's protected health information, such as the hardware (computers, scanners, *etc.*) or software that is used to generate an electronic copy of an individual's protected health information in response to an access request. We note this limitation is in contrast to a covered entity's ability to charge for supplies for hard copies of protected health information (*e.g.,* the cost of paper, the prorated cost of toner and wear and tear on the printer). *See* 65 FR 82462, 82735, Dec. 28, 2000 (responding to a comment seeking clarification on "capital cost for copying" and other supply costs by indicating that a covered entity was free to recoup all of their reasonable costs for copying). We believe this interpretation is consistent with the fact that, unlike a hard copy, which generally exists on paper, an electronic copy exists independent of media, and can be transmitted securely via multiple methods (*e.g.,* e-mail, a secure Web-based portal, or an individual's own electronic media) without accruing any ancillary supply costs.

We also note, however, that our interpretation of the statute would permit a covered entity to charge a reasonable and cost-based fee for any electronic media it provided, as requested or agreed to by an individual who does not provide their own. For example, a covered entity can offer to make protected health information available on an encrypted USB flash drive, and can charge a reasonable cost-based fee for the flash drive. If, however, an individual has brought his or her own electronic media (such as a recordable CD), requested that an electronic copy be placed on it, and the covered entity's systems are readily able to do so, then the covered entity would not be allowed to require the individual to purchase an encrypted USB flash drive instead. Likewise, if an individual requests that an electronic copy be sent via unencrypted e-mail, the covered entity should advise the individual of the risks associated with unencrypted e-mail, but the covered entity would not be allowed to require the individual to instead purchase a USB flash drive.

While we propose to renumber the remaining factors in § 164.524(c)(4), we

do not propose to amend their substance. With respect to § 164.524(c)(4)(iii), however, we note that our interpretation of the statute would permit a covered entity to charge for postage if an individual requests that the covered entity transmit portable media containing an electronic copy through mail or courier (*e.g.,* if the individual requests that the covered entity save protected health information to a CD and then mail the CD to a designee).

Finally, we are requesting comment on one aspect of the right to access and obtain a copy of protected health information which the HITECH Act did not amend. In particular, the HITECH Act did not change the timeliness requirements for provision of access in § 164.524(b). Under the current requirements, a request for access must be approved or denied, and if approved, access or a copy of the information provided, within 30 days of the request. In cases where the records requested are only accessible from an off-site location, the covered entity has an additional 30 days to respond to the request. In extenuating circumstances where access cannot be provided within these timeframes, the covered entity may have a one-time 30-day extension if the individual is notified of the need for the extension within the original timeframes.

With regard to the timeliness of the provision of access, we are aware that with the advance of electronic health records, there is an increasing expectation and capacity to provide individuals with almost instantaneous electronic access to the protected health information in those records through personal health records or similar electronic means. On the other hand, we are not proposing to limit the right to electronic access of protected health information to certified electronic health records, and the variety of electronic systems that are subject to this proposed requirement would not all be able to comply with a timeliness standard based on personal health record capabilities. It is our assumption that a single timeliness standard that would address a variety of electronic systems, rather than having a multitude of standards based on system capacity, would be the preferred approach to avoid workability issues for covered entities. Even under a single standard, nothing would prevent electronic health record systems from being developed through the HITECH Act's standards and certification process with the technological capabilities to exceed the Privacy Rule's timeliness requirements for providing access to individuals. Based on the assumption that a single standard would be the preferred approach, we are interested in public comment on an appropriate, common timeliness standard for the provision of access by covered entities with electronic designated record sets generally. We would appreciate comment on aspects of existing systems that would create efficiencies in processing of requests for electronic information, as well as those aspects of electronic systems that would provide little change from the time required for processing a paper record. Alternatively, we request comment on whether the current standard could be altered for all systems, paper and electronic, such that all requests for access should be responded to without unreasonable delay and not later than 30 days.

We are also interested in public comment on whether, contrary to our assumption, a variety of timeliness standards based on the type of electronic designated record set is the preferred approach and if so, how we should operationalize such an approach. For example, how should we identify and characterize the various electronic designated record sets to which the different standards would apply, such as personal health records, electronic health records, and others? What functionality within these electronic systems would drive the need for more or less time to provide an individual with electronic access? What timeliness standards would be appropriate for the different systems? What timeliness standard(s) would be required of entities with protected health information spread across hybrid systems that have different functionalities? What would be the impact of and challenges to having multiple timeliness standards for access?

Finally, we request comment on the time necessary for covered entities to review access requests and make necessary determinations, such as whether the granting of access would endanger the individual or other persons so as to better understand how the time needed for these reviews relates to the overall time needed to provide the individual with access. Further, we request comment generally on whether the provision which allows a covered entity an additional 30 days to provide access to the individual if the protected health information is maintained off-site should be eliminated altogether for both paper and electronic records, or at least for protected health information maintained or archived electronically because the physical location of electronic data storage is not relevant to its accessibility.

L. Other Technical and Conforming Changes

We propose to make a number of technical and conforming changes to the Privacy Rule to fix minor problems such as incorrect cross-references, mistakes of grammar, and typographical errors. Technical and conforming changes of this nature are described and explained in the table below.

Regulation §	Current language	Proposed change	Reason for change
164.510(b)(2)(iii)	"based the exercise of professional judgment".	Insert "on" after "based"	Correct typographical error.
164.512(b)(1)	"Permitted disclosures" and "may disclose".	Insert "uses and" and "use or" before "disclosures" and "disclose," respectively.	Correct inadvertent omission.
164.512(e)(1)(iii)	"seeking protecting health information".	Change "protecting" to "protected"	Correct typographical error.
164.512(e)(1)(vi)	"paragraph (e)(1)(iv) of this section"	Change "(e)(1)(iv)" to "(e)(1)(v)"	Correct cross-reference.
164.512(k)(3)	"authorized by 18 U.S.C. 3056, or to foreign heads of state . . ., or to for the conduct of investigations".	Remove the comma after "U.S.C. 3056" and the "to" before "for".	Correct typographical errors.

In addition to the technical changes listed in the table above, we propose to make a few changes that are technical or conforming in nature, but for which the reason for the change is more programmatic in nature. These are as follows:

Section 164.506(c)(5) permits a covered entity to disclose protected health information "to another covered entity that participates in the organized health care arrangement." We propose to change the words "another covered entity that participates" to "other participants" because not all participants in an organized health care arrangement may be covered entities; for example, some physicians with staff privileges at a hospital may not be covered entities.

Section 164.510(a)(1)(ii) permits the disclosure of directory information to members of the clergy and other persons who ask for the individual by name. We propose to add the words "use or" to this permission, to cover the provision of such information to clergy who are part of a facility's workforce.

Section 164.510(b)(3) covers uses and disclosures of protected health information when the individual is not present to agree or object to the use or disclosure, and, as pertinent here, permits disclosure to persons only of "the protected health information that is directly relevant to the person's involvement with the individual's health care." We propose to delete the last two quoted words and substitute therefore the following: "care or payment related to the individual's health care or needed for notification purposes." This change would align the text of paragraph (b)(3) with the permissions provided for at paragraph (b)(1) of this section.

Where an employer needs protected health information to comply with workplace medical surveillance laws, such as OSHA or MSHA, § 164.512(b)(1)(v)(A) permits a covered entity to disclose, subject to certain conditions, protected health information of an individual to the individual's employer if the covered entity is a covered health care provider "who is a member of the workforce of such employer or who provides health care to the individual at the request of the employer." We propose to amend the quoted language by removing the words "who is a member of the workforce of such employer or", as the language is unnecessary.

In § 164.512(k)(1)(ii), we propose to replace the word "Transportation" with "Homeland Security." The language regarding a component of the Department of Transportation was included to refer to the Coast Guard; however, the Coast Guard was transferred to the Department of Homeland Security in 2003. In addition, at § 164.512(k)(5)(i)(E), we propose to replace the word "and" after the semi-colon with the word "or." The intent of § 164.512(k)(5)(i) is not that the existence of all of the conditions is necessary to permit the disclosure, but rather that the existence of any would permit the disclosure.

VII. Regulatory Analyses

A. Introduction

We have prepared a regulatory impact statement in compliance with Executive Order 12866 (September 1993, Regulatory Planning and Review), the Regulatory Flexibility Act (RFA) (September 19, 1980, Pub. L. 96–354), the Unfunded Mandates Reform Act of 1995 (Pub. L. 104–4), and Executive Order 13132 on Federalism.

1. Executive Order 12866

Executive Order 12866 directs agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). A regulatory impact analysis must be prepared for major rules that have economically significant effects ($100 million or more in any one year) or adversely affect in a material way the economy, a sector of the economy, productivity, competition, jobs, the environment, public health or safety, or State, local, or Tribal government or communities (58 FR 51741).

We estimate that the effects of the requirement for covered entities (including indirect costs incurred by third party administrators, which frequently send out notices on behalf of health plans) to issue new notices of privacy practices, will result in new costs of $166.1 million within 12 months of the effective date of the final rule. We estimate that the private sector will bear approximately 71 percent of the costs, with State and Federal plans bearing the remaining 29 percent of the costs. As a result of the economic impact, and other costs that are expected but not quantified in the regulatory analysis below, we determined that this proposed rule is an economically significant regulatory action within the meaning of section 3(f)(4) of Executive Order 12866. We present our analysis of the costs of the proposed rule in section C below.

2. Regulatory Flexibility Act

The RFA requires agencies to analyze options for regulatory relief of small businesses if a rule has a significant impact on a substantial number of small entities. We present our regulatory flexibility analysis of this proposed rule in section E below.

The Act generally defines a "small entity" as (1) a proprietary firm meeting the size standards of the Small Business Administration (SBA), (2) a nonprofit organization that is not dominant in its field, or (3) a small government jurisdiction with a population of less than 50,000. Because 90 percent or more of all health care providers meet the SBA size standard for a small business or are nonprofit organizations, we generally treat all health care providers as small entities for purposes of performing a regulatory flexibility analysis. The SBA size standard for health care providers ranges between $7.0 million and $34.5 million in annual receipts.

With respect to health insurers and third party administrators, the SBA size standard is $7.0 million in annual receipts. While some insurers are classified as nonprofit, it is possible they are dominant in their market. For example, a number of Blue Cross/Blue Shield insurers are organized as nonprofit entities; yet they dominate the health insurance market in the States where they are licensed. In addition, we lack the detailed information on annual receipts for insurers and plan administrators and, therefore, we do not know how many firms qualify as small entities. We welcome comments on the number of small entities in the health insurer and health plan administrator market.

3. Unfunded Mandates Reform Act

Section 202 of the Unfunded Mandates Reform Act of 1995 (UMRA) requires that agencies assess anticipated costs and benefits before issuing any rule whose mandates would require spending in any one year $100 million in 1995 dollars, updated annually for inflation. In 2010, that threshold is approximately $135 million. UMRA does not address the total cost of a rule. Rather, it focuses on certain categories of cost, mainly those "Federal mandate" costs resulting from: (1) Imposing enforceable duties on State, local, or Tribal governments, or on the private sector; or (2) increasing the stringency of conditions in, or decreasing the funding of, State, local, or Tribal governments under entitlement programs.

We are able to identify approximately $166.1 million in costs on both the private sector and State and Federal health plans. There may be other costs we are not able to monetize because we lack data, and the proposed rule may produce savings that may offset some or all of the added costs. For this purpose, we must also separately identify costs to

be incurred by the private sector and those incurred by State and Federal entities.

As noted above, of the costs we can identify, we estimate that approximately 71 percent or $118.1 million of new costs will fall on the private sector. For the purpose of this calculation, we included all $46 million in provider costs as private sector costs. While we recognize that some providers are State or Federal entities, we do not have adequate information to estimate the number of public providers, but we believe the number to be significantly less than 10% of all providers shown in Table 1. Therefore, as we did for the RFA analysis and for ease of calculation, we assumed that all provider costs are private sector costs. We welcome comment on this assumption and any information regarding the number of the public sector providers for future analysis. With regard to identifying the costs to private sector health plans, based on the data discussed in section C below, we estimate that 60 percent of policy holders are served by private sector health plans and, therefore, have allocated 60 percent of the costs to be incurred by all health plans as private sector costs, or $72.1 million.

Similarly, we estimate that approximately 29 percent or $48 million of the new costs will fall on State and Federal plans. As noted above, based on the data discussed in section C below, we estimate that 40 percent of policy holders are served by public sector plans and, therefore, have allocated 40 percent of the costs for all health plans as public sector costs, or $48 million. Because the amount of unfunded mandates incurred separately by either the private sector or by State, local, and Tribal governments will not exceed the unfunded mandates threshold of $133 million, we are not required to perform a cost-benefit analysis under the UMRA. Nonetheless, we have prepared a cost-benefit analysis of the proposed rule in sections C and D, below, as required by Executive Order 12866 for an economically significant regulation. We welcome public comment on the analysis as it bears upon our assumptions and calculations under the UMRA.

4. Federalism

Executive Order 13132 establishes certain requirements that an agency must meet when it promulgates a proposed rule (and subsequent final 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 and Security Rules were assessed as required by Executive Order 13132 and published as part of the preambles to the final rules on December 28, 2000 (65 FR 82462, 82797) and February 20, 2003 (68 FR 8334, 8373), respectively. Regarding preemption, the preamble to the final Privacy Rule explains that the HIPAA statute dictates the relationship between State law and Privacy Rule requirements, and the Rule's preemption provisions do not raise Federalism issues. The HITECH Act, at section 13421(a), provides that the HIPAA preemption provisions shall apply to the HITECH provisions and requirements. While we have made minor technical changes to the preemption provisions in Subpart B of Part 160 to conform to and incorporate the HITECH Act preemption provisions, these changes do not raise new Federalism issues. The proposed changes include: (1) Amending the definitions of "contrary" and "more stringent" to reference business associates; and (2) further amending the definition of contrary to provide that State law would be contrary to the HIPAA Administrative Simplification provisions if it stands as an obstacle to the accomplishment and execution of the full purposes and objectives of not only HIPAA, but also the HITECH Act.

We do not believe that this rule will impose substantial direct compliance costs on State and local governments that are not required by statute. It is our understanding that State and local government covered entities do not engage in marketing, the sale of protected health information, or fundraising. Therefore, the proposed modifications in these areas would not cause additional costs to State and local governments. We anticipate that the most significant direct costs on State and local governments will be the cost for State and local government-owned covered entities of drafting, printing, and distributing revised notices of privacy practices, which would include the cost of mailing these notices for State health plans, such as Medicaid. However, the costs involved can be attributed to the statutory requirements.

In considering the principles in and requirements of Executive Order 13132, the Department has determined that these proposed modifications to the Privacy and Security Rules will not significantly affect the rights, roles, and responsibilities of the States.

B. Why is This Rule Needed?

The proposed rule is needed to implement several provisions of the HITECH Act that require us to amend our regulations at 45 CFR Parts 160 and 164. These amendments primarily strengthen the privacy and security protections for protected health information, as well as broaden the privacy rights of individuals.

C. Costs

1. Notifying Individuals of Their New Privacy Rights

Covered entities must provide individuals with NPPs that detail how the covered entity may use and disclose protected health information and individuals' rights with respect to their own health information. Due to the proposed modifications pursuant to the HITECH Act, covered entities must modify their NPPs and distribute them to affected individuals to advise them of the following strengthened privacy protections: (1) The addition of the sale of protected health information as a use or disclosure that requires the express written authorization of the individual; (2) a separate statement that provides advance notice to the individual if the healthcare provider receives financial remuneration from a third party to send treatment communications to the individual about that party's products or services, and the right of the individual to elect not to receive such communications; and (3) the right of the individual to restrict disclosures of protected health information to a health plan with respect to treatment services for which the individual has paid out of pocket in full.

For providers, the cost of developing a new NPP consists of drafting and printing the notice. The costs of distribution are minimal because providers will hand out the NPPs when patients come for their appointments. We estimate that drafting the updated NPPs will require approximately one-third of an hour of professional, legal time at approximately $90 per hour—or $30—that includes hourly wages of $60 plus 50 percent [5]. The total cost for attorneys for the approximately 697,000 [6] health care providers in the

[5] *http://www.bls.gov/oes/2008/may/oes231011.htm* for lawyers.

[6] We identified 701,325 entities that must prepare and deliver NPPs that are shown in Table 1 below. This includes 696,758 HIPAA covered entities that are health care providers, including hospitals, nursing facilities, doctor offices, outpatient care centers, medical diagnostic, imaging service, home health service and other ambulatory care service covered entities, medical equipment suppliers, and pharmacies. For the purposes of our calculation, we have rounded this number to 697,000. Table 1 also includes 4,567 health insurance carriers and third party administrators working on behalf of covered health plans. The cost estimates for these entities are addressed later.

U.S. is, therefore, expected to be approximately $21 million. Printing the NPPs will require paper and clerical time at a cost of $0.10 per notice. We estimate that within 12 months from the effective date of the final rule, providers will print approximately 250 million NPPs to hand to patients who visit their offices. Printing costs for 250 million NPPs will be $25 million. The total cost for providers is approximately $46 million.

For health plans, the cost of developing a new NPP consists of drafting, printing and mailing the notice. With the exception of a few large health plans, most health plans do not self-administer their plans. The majority of plans are either health insurance issuers (approximately 1,000) or utilize third party administrators that act on their behalf in the capacity as business associates. We identified approximately 3,500 third party administrators acting as business associates for approximately 446,400 ERISA plans identified by the Department of Labor. In addition, the Department of Labor identified 20,300 public non-Federal health plans that may use third party administrators. Almost all of the public and ERISA plans, we believe, employ third party administrators to administer their health plans. While the third party administrators will bear the direct costs of issuing the revised NPPs, the costs will generally be passed on to the plans that contract with them. Those plans that self-administer their own plans will also incur the costs of issuing the revised NPPs. We do not know how many plans administer as well as sponsor health plans and invite comments on the number of self-administered plans; however, unless there were many such plans it would not have much effect on these estimates.

For the approximately 4,500 health insurance issuers and health plan administrators, the cost of composing and printing the NPPs will be a similar amount per NPP to the amount calculated for providers. However, health insurers and plan administrators will have to mail the NPPs to policy holders. The costs for the mailing will consist of postage and clerical time. The cost, therefore, depends on the estimate of the number of policy holders who must receive NPPs. We did not assume that health plans would communicate with policy holders by e-mail because we have no data that indicate the extent to which insurance plans and third party administrators communicate currently with their policy holders through e-mail. We request public comment on this assumption.

Because the Privacy Rule requires that only the named insured or policy holder be notified of changes to the health plans' privacy practices even if that policy also covers dependents, we expect that only policy holders will receive the revised NPPs mandated by this rule. For public programs such as Medicare, where each individual is a policy holder, Medicare has a policy of mailing one notice or a set of program materials to a household of four or fewer beneficiaries at the same address. Although there are 45.6 million individual Medicare beneficiaries, the program only sends out 38.8 million pieces of mail per mailing.

Actuarial Research Corporation (ARC), our consultant, estimated the number of policy holders for all classes of insurance products to be approximately 183.6 million, including all public programs. The data comes from the Medical Expenditure Panel Survey from 2004–2006 projected to 2010. ARC estimated 112.6 million private sector policy holders and 71.0 million public "policy holders." The total, including more recent Medicare data, is 188.3 million persons (which results in roughly a split of 60 percent private policy holders and 40 percent public "policy holders"), whom we expect to receive NPPs from their plans. The estimates do not capture policy holders who are in hospitals or nursing homes at the time of the survey, or individuals who may have been insured under more than one plan in a year, for example, because their job status changed, they have supplemental policies, or they have more than one employer, creating duplicate coverage. Therefore, ARC recommended we use 200 million for the number of NPPs that will actually be sent.

The costs of drafting, printing, and distributing the NPP are estimated to be the following. First, drafting the NPP is estimated to require one-third hour of legal services at a cost of $30 × 4,500 insurance plans and insurance administrative entities, which equals $135,000. Second, the cost of printing the NPP, which includes the cost of paper and actual printing, is estimated to be $0.10 per notice × 200 million notices, which equals $20 million. Third, the cost of distributing the NPPs would involve clerical time to prepare the mailings and the cost of postage, which we estimate to be a unit cost of $0.50 per NPP for postage and handling using the rate of $0.44 per stamp and $0.06 for labor (the same rates we used in the Breach Notification for Unsecured Protected Health Information Regulations published in the **Federal Register** at 74 FR 42763), results in an estimated $100 million cost for distribution. The total cost for all plans for drafting, printing, and distributing the NPP therefore, is approximately $120.1 million. We note that this total may be an overestimation of the costs because many insurers may use bulk mailing rates to distribute their NPPs which would reduce their mailing costs.

The total estimated cost for both providers and health plans to notify individuals and policy holders of changes in their privacy rights is approximately $166.1 million in the first year following implementation of the rule. Annualized over 10 years at three percent and seven percent, the cost equals $194,720 and $236,489, respectively.

Table 1 below shows the number of covered entities by class of provider and insurer that would be required to issue NPPs under the proposed rule.

TABLE 1—NUMBER OF ENTITIES BY NAICS CODE[1] EXPECTED TO PREPARE AND DISTRIBUTE REVISED NPPS

NAICS	Providers/Suppliers	Entities
622	Hospitals (General Medical and Surgical, Psychiatric, Substance Abuse, Other Specialty)	4,060
623	Nursing Facilities (Nursing Care Facilities, Residential Mental Retardation Facilities, Residential Mental Health and Substance Abuse Facilities, Community Care Facilities for the Elderly, Continuing Care Retirement Communities).	34,400
6211–6213	Office of MDs, DOs, Mental Health Practitioners, Dentists, PT, OT, ST, Audiologists	419,286
6214	Outpatient Care Centers (Family Planning Centers, Outpatient Mental Health and Drug Abuse Centers, Other Outpatient Health Centers, HMO Medical Centers, Kidney Dialysis Centers, Freestanding Ambulatory Surgical and Emergency Centers, All Other Outpatient Care Centers).	13,962
6215	Medical Diagnostic, and Imaging Service Covered Entities	7,879
6216	Home Health Service Covered Entities	15,329
6219	Other Ambulatory Care Service Covered Entities (Ambulance and Other)	5,879
n/a	Durable Medical Equipment Suppliers[2]	107,567

TABLE 1—NUMBER OF ENTITIES BY NAICS CODE[1] EXPECTED TO PREPARE AND DISTRIBUTE REVISED NPPS—Continued

NAICS	Providers/Suppliers	Entities
4611	Pharmacies[3]	88,396
524114	Health Insurance Carriers	1,045
524292	Third Party Administrators Working on Behalf of Covered Health Plans	3,522
	Total Entities	701,325

[1] Office of Advocacy, SBA, *http://www.sba.gov/advo/research/data.html.*
[2] Centers for Medicare & Medicaid Services covered entities.
[3] The Chain Pharmacy Industry *http://www.nacds.org/wmspage.cfm?parm1=507.*

2. Authorization and Other Requirements for Disclosures Related to Marketing and Sale of Protected Health Information

The proposed rule would make modifications to the definition of "marketing," such that some communications to individuals about health-related products or services that are made under health care operations would now be considered marketing communications if the covered entity receives financial remuneration by a third party to make the communication. For marketing communications, individual authorization is required. In addition, the proposal would require that a health care provider that receives financial remuneration by a third party in exchange for sending a treatment communication to an individual about the third party's product or service must disclose the fact of remuneration in the communication and provide the individual with a clear and conspicuous opportunity to opt out of receiving future subsidized communications. Although this proposed rule would modify the current definition of "marketing," because we do not have information on the extent to which covered entities currently receive financial remuneration from third parties in exchange for sending information to individuals about the third parties' health-related products or services, we do not know how these modifications would change how covered entities operate. We invite public comment on this issue.

In addition, the proposed rule would require an individual authorization before a covered entity could disclose protected health information in exchange for remuneration (*i.e.,* "sell" protected health information). The proposal includes several exceptions to this authorization requirement. On its face, this proposed modification would appear to increase the burden to covered entities by requiring them to obtain authorizations in situations in which no authorization is currently required. However, we believe such a scenario is unlikely to occur. Even if covered entities attempted to obtain authorizations in compliance with the proposed modifications, we believe most individuals would not authorize these types of disclosures. It would not be worthwhile for covered entities to continue to attempt to obtain such authorizations, and as a result, we believe covered entities would simply discontinue making such disclosures. Therefore, we believe this proposed modification would have little to no impact on covered entities. We request comment on this issue.

The proposed provision requiring individual authorization prior to the sale of protected health information contains several exceptions in which protected health information could be disclosed in exchange for remuneration without first obtaining individual authorization. Most of the excepted disclosures would not impose additional requirements and, therefore, would not impose any additional burden on covered entities to implement. However, the exception for research disclosures may impose an additional burden on researchers. The exception applies to disclosure of protected health information for research as long as the remuneration received does not exceed the cost to produce and transmit the information. Researchers who purchase data from covered entities may now incur additional costs as a result of the proposed rule, in order to obtain newly required authorizations, if they are currently paying a covered entity more than the cost to produce and transmit the protected health information (unless the covered entity is willing to reduce its charges for the data). The proposed change would classify such transactions as a sale, and as such would require an individual's authorization prior to the covered entity's disclosure. This authorization requirement also may have additional effects on research, such that the need for authorization may skew the sample, or if the researcher does not have the resources to obtain the authorizations from the research subjects, the research may be jeopardized. Since we have no information on the amounts currently paid to covered entities by researchers for protected health information, we have no way to estimate the impact of the provision. We welcome any comments and information on the impact of these provisions.

3. Authorization for Compound Disclosures

The proposed rule would permit compound authorizations for research purposes as long as it is clear to individuals that they do not have to agree to both the conditioned and unconditioned components of an authorization in order to receive research-related treatment. We believe that the proposed provision would reduce burden on the research community by eliminating the need for multiple forms for research studies involving both a clinical trial and a related research repository or study. However we have no data which would permit us to estimate the amount of burden reduction associated with this proposal. We welcome public comment on this issue.

4. Uses and Disclosures of Decedents' Protected Health Information

The proposed rule would modify the current rule to limit the period for which a covered entity must protect an individual's health information to 50 years after the individual's death. We believe this will reduce the burden on both covered entities and on those seeking the protected health information of persons who have been deceased for many years by eliminating the need to search for and find a personal representative of the decedent, who in many cases may not be known or even exist after so many years, to authorize the disclosure. We believe this change would benefit family members and historians who may seek access to the medical information of these decedents for personal and public interest reasons. However, we lack any data to be able to estimate the benefits or costs of this

provision. We welcome comments on this proposed change.

5. Uses and Disclosures for Care and Notification Purposes

The proposed rule would permit covered entities to disclose a decedent's protected health information to family members, or other persons involved in the individual's care or payment for care before the individual's death, unless doing so would be inconsistent with any prior expressed preference of the individual that is known to the covered entity. The rights of the decedent's personal representative to have access to the protected health information of the decedent would remain unchanged. We believe the proposed change would reduce burden by permitting covered entities to continue to disclose protected health information to family members and other persons who were involved in an individual's care while the individual was alive after the death of the individual without needing to obtain authorization from the decedent's personal representative, who may not be known or even exist. However, we have no data to permit us to estimate the reduction in burden and we welcome comment on this change.

6. Public Health Disclosures

The proposed rule would create a new public health provision to permit disclosure of proof of a child's immunization by a covered entity to a school in States that have school entry or similar laws. This proposed change would allow a covered health care provider to release proof of immunization to a school without having to obtain a written authorization, provided the provider obtained the agreement (oral or otherwise) to the disclosure from either the parent or guardian, or the individual, if the individual is an adult or emancipated minor. We expect the proposed change to the regulations may reduce the burden on covered entities and parents in obtaining and providing written authorizations but it is unclear by how much. Since the proposed rule would require the covered entity and the responsible party for the student to agree that the covered entity may release proof of immunization, some covered entities may request the agreement in writing. In these cases, there may be little change from the current authorization requirement in terms of the burden. Because we lack data on the burden reduction, we cannot provide an estimate of the possible savings. We welcome comment on the proposed change.

7. Fundraising Requirements

The proposed rule would require that any fundraising communication sent to an individual must provide the recipient with a clear and conspicuous opportunity to opt out of receiving any further fundraising communications. If an individual elects to opt out, the fundraising entity must not send that individual additional fundraising communications. We believe that the strengthened language from the HITECH Act that requires fundraisers to clearly and conspicuously provide the recipient an opt-out choice from receiving future communication and to treat such a choice as a revocation of authorization will result in fewer unwanted fundraising communications. However, we lack the data to estimate the effects of this change. We request comment on the extent to which the requirement that the opportunity to elect not to receive further fundraising communications be clear and conspicuous would have an impact on covered entities and their current fundraising materials.

8. Individuals' Access to Protected Health Information

Under the proposed regulations, if a covered entity maintains protected health information electronically and the recipient requests copies of his or her protected health information in an electronic format, the covered entity or business associate must provide the information in the electronic format requested by the individual if readily producible in that format, or, if not, in a different electronic format agreed to by the covered entity and the individual. If the covered entity provides an individual with electronic access to protected health information, the proposed rule would only allow the covered entity to charge the costs of labor associated with the preparation of the request. The proposed rule clarifies the labor and supply costs applicable to preparation of electronic requests vs. paper requests. Labor costs to produce an electronic copy involve the cost of reviewing and preparing the copy. Supplies for an electronic copy apply only to the cost of the media, if applicable, for providing the information to the individual. If the individual provides the media (*e.g.,* a CD or flash drive), there would be no cost for the media. Similarly, if the information is transmitted via e-mail or some other electronic mode, there would be no charge for media.

It is unclear whether there will be any cost increase or decrease to either the individual or the covered entity with respect to the individual's increased access to their electronic protected health information. The fact that the proposed rule requires the covered entity to provide information in an electronic format may be, in practice, no different than the current requirement to provide protected health information to the individual in electronic format, if readily producible in such format. Both the current and proposed rules continue to permit the covered entity and individual to negotiate over the format and delivery of protected health information. By emphasizing the provision of protected health information electronically, the proposed rule may lower costs because postage costs are eliminated or reduced and labor and supply costs are significantly reduced. In conclusion, there may be some savings that result from the greater use of electronic access to protected health information, but we cannot quantify them.

9. Business Associates and Covered Entities and Their Contractual Relationships

The proposed rule would extend liability for failure to comply with the Privacy and Security Rules directly to business associates and business associate subcontractors in a manner similar to how they now apply to covered entities. The proposed rule would subject business associates to many of the same standards and implementation specifications, and to the same penalties, that apply to covered entities under the Security Rule and to some of the same standards and implementation specifications, and to the same penalties, that apply to covered entities under the Privacy Rule. Additionally, business associates would also be required to obtain satisfactory assurances in the form of a business associate agreement from subcontractors that the subcontractors will safeguard any protected health information in their possession. If the business associate learns of a pattern of activity or practice of a subcontractor that constitutes a material breach or violation of the contract, the business associate would be required to make reasonable attempts to repair the breach or correct the violation. If unsuccessful, the business associate would be required to terminate the contract, if feasible. In addition, a business associate would be required to furnish any information the Secretary requires to investigate whether the business associate is in compliance with the regulations.

In the absence of reliable data to the contrary, we assume that business associates' compliance with their

contracts range from the minimal compliance to avoid contract termination to being fully compliant. The burden of the proposed rules on business associates depends on the terms of the contract between the covered entity and business associate, and the degree to which a business associate established privacy policies and adopted security measures that comport with the HIPAA Rules. For business associates that have already taken HIPAA-compliant measures to protect the privacy and security of the protected health information in their possession, the proposed rules with their increased penalties would impose limited burden.

We assume that business associates in compliance with their contracts would have already designated personnel to be responsible for formulating the organization's privacy and security policies, performed a risk analysis, and invested in hardware and software to prevent and monitor for internal and external breaches of protected health information. We expect that most business associates make a good-faith effort to follow the terms of their contracts and comply with current security and privacy standards.

For those business associates that have not already adopted HIPAA-compliant privacy and security standards for protected health information, the risk of criminal and/or civil monetary penalties may spur them to increase their efforts to comply with the privacy and security standards. Up to this point, the consequences of failing to meet the privacy and security standards were limited to a business loss in the form of a terminated contract. In the context of the business associate's overall business, the risk of losing the contract may not be a sufficient incentive to warrant investing in added security or establishing privacy policies potentially at significant expense. There may be other more benign reasons such as ignorance of potential threats or lack of knowledgeable personnel on staff. Regardless of the reason, to avoid the risk of the far more serious penalties in this proposed rule, we expect that business associates and subcontractors that have been lax in their complying with the privacy and security standards may now take steps to enhance their security procedures and strengthen their policies for protecting the privacy of the protected health information under their control.

As stated above, we have no information on the degree of contract enforcement and compliance among business associates. We also lack information regarding the size or type of business associates that contract with covered entities. We have only rough estimates as to the overall number of business associates, which ranges from approximately one million to two million depending upon the number of business associates which serve multiple covered entities. As the area of health information technology expands, we note that the proposed rule also includes in the definition of business associates entities such as e-prescribing gateways, health information organizations or other organizations that provide data transmission services with respect to protected health information to a covered entity.

As a result of the lack of information, we can only assume that some business associates and subcontractors comply with existing privacy and security standards. For them, the proposed rules would impose only a limited burden. For business associates that do not have HIPAA-compliant privacy policies and security procedures, the proposed rules imposing criminal and civil monetary penalties directly on business associates and their subcontractors may incentivize these organizations to bolster their security and privacy policies. Depending on the current level of compliance, for some business associates, the proposed rule could impose significant burdens. We welcome comments on our analysis and especially invite information regarding the amount of burden and the number of affected business associates.

The cost to renegotiate contracts between covered entities and business associates and between business associates and subcontractors may be minimal if we assume that all parties are living up to their current contractual agreements. At the same time, we anticipate that an unknown number of contracts will have to be modified to reflect the changes in law and in the rules we propose. The time involved in modifying a contract is estimated to be one hour of a legal professional's time. Based on the Bureau of Labor Statistics reports, the average hourly wage of $60 plus an estimated additional 50 percent for benefits brings the hourly rate to $90.

Because we are allowing contracts to be phased in over one year from the compliance date or 18 months from the effective date of the final rule, we expect that the costs of modifying contracts will be incorporated into the normal renegotiation of contracts as the contracts expire. We believe that most contracts will be renegotiated over the phase-in period. In addition, the Department expects to issue revised sample business associate contract language when these rules are finalized, which may help to lessen the costs associated with contract modifications. Under these assumptions, the costs will be minimal. We request comments on the number of contracts and covered entities that will not be able to complete renegotiation of their contracts with their business associates within 18 months.

Even with the phase-in period for renegotiating contracts, we expect there will be an unknown number of covered entities and business associates that will have to renegotiate their contracts before the term of their current contracts expire because: (1) some contracts may extend beyond the eighteen month period, (2) fear of incurring civil or criminal penalties may motivate the parties to ensure they are in compliance with the new rules, and (3) the covered entity and business associate may have established only the minimum requirements and seek to strengthen their compliance under the new rules.

As stated previously, we are unsure which of these scenarios applies. We welcome comments on the extent of cost to renegotiate contracts.

D. Benefits

The proposed modifications pursuant to the HITECH Act would provide benefits to individuals. The benefits for individuals include added information on their rights through an expanded NPP and greater control over the uses and disclosures of their personal health information by expanding the requirements to obtain authorization before a covered entity or business associate can disclose their protected health information in exchange for remuneration and to restrict certain disclosures at the request of the individual. Under the proposed rule, individuals would also have easier access to their protected health information in an electronic format, and relatives and friends of deceased persons would be able to obtain the person's protected health information when there is no personal representative or without obtaining authorization under some circumstances. In addition, covered entities would only need to protect the health information of decedents for 50 years after their death, as opposed to protecting the information in perpetuity as is required by the current rule. This would also mean that the personal health information of persons who had been deceased for many years would be available to historians, researchers, and family members. Also, individuals' rights with respect to fundraising communications would be strengthened. In States that

require immunization information for school attendance, schools would have an easier time obtaining immunization records because the proposed rule would eliminate the need for written authorization.

Under the proposed rule, pursuant to the HITECH Act, an individual's health information will be afforded greater protection since business associates of covered entities would share responsibility with the covered entity for safeguarding against impermissible disclosures of protected health information. Business associates and subcontractors would be subject to criminal and civil penalties for violating the privacy and security of protected health information entrusted to them.

While we are certain that the proposed regulatory changes represent distinct benefits, we cannot monetize their value. We have no measure for valuing the benefit an individual would gain from the authorization requirement when a covered entity or business associate exchanges protected health information for remuneration. Neither do we know how much value would be added when an individual receives their protected health information in an electronic format nor the amount of time saved as a result of the public health disclosure provision for student immunizations. Also, the value that relatives and friends of a deceased person would gain from obtaining the protected health information of the decedent that they would not otherwise be able to obtain because there is no personal representative or, if there is a personal representative, without the delay of obtaining authorization, is beyond our ability to measure. We welcome comments and information that could improve our analysis of the benefits of the proposed rule.

E. Regulatory Flexibility Analysis

The Regulatory Flexibility Act requires agencies that issue a proposed rule to analyze and consider options for reducing regulatory burden if the regulation will impose a significant burden on a substantial number of small entities. The Act requires the head of the agency to either certify that the rule would not impose such a burden or perform a regulatory flexibility analysis and consider alternatives to lessen the burden.

The proposed rule would have an impact on covered providers of health care, health insurance issuers, and third party administrators acting on behalf of health plans, which we estimate to total 701,325. Of the approximately $166.1 million in costs we are able to identify, the private sector will incur approximately 71 percent of the costs or $118.1 million. The average cost per covered entity is therefore approximately $168. We do not view this as a significant burden. We note that the 3,500 third party administrators included in this calculation serve as business associates to the approximately 446,000 ERISA plans, most of which are small entities. We have no information on how many of these plans self-administer, and we request any data the public may provide on this question. Based on the relatively small cost per covered entity, the Secretary certifies that the proposed rule would not have a significant impact on a substantial number of small entities. However, because we are not certain of all the costs this rule may impose or the exact number of small health insurers or third party administrators, we welcome comments that may further inform our analysis.

Although we certify that the proposed rule will not impose a significant burden on a substantial number of small entities, in drafting the proposed provisions of the rule, we considered alternatives for reducing the burden on small entities.

First, in the rule we are proposing to allow covered entities and business associates with existing HIPAA compliant contracts twelve months from the compliance date to renegotiate their contracts unless the contract is renewed or modified before such date. This amount of time plus the six months from the effective date of the rule to the compliance date generally gives the parties 18 months to renegotiate their agreements. We believe that the added time will reduce the cost to revise agreements because the changes the rule requires will be incorporated into the routine updating of covered entities and business associates contracts.

Second, as we did in the final Privacy Rule published August 14, 2002 (67 FR 53182, 53264–53266) we will provide sample language for revising the contracts between covered entities and business associates. While the language is generic and may not suit complex organizations with complex agreements, we believe that it will help small entities with their contract revisions and save them time and money in redrafting their contracts to conform to the new rules.

VIII. Collection of Information Requirements

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

a. Whether the information collection is necessary and useful to carry out the proper functions of the agency;

b. The accuracy of the agency's estimate of the information collection burden;

c. The quality, utility, and clarity of the information to be collected; and

d. Recommendations to minimize the information collection burden on the affected public, including automated collection techniques.

Under the PRA, the time, effort, and financial resources necessary to meet the information collection requirements referenced in this section are to be considered. We explicitly seek, and will consider, public comment on our assumptions as they relate to the PRA requirements summarized in this section. To comment on this collection of information or to obtain copies of the supporting statement and any related forms for the proposed paperwork collections referenced above, e-mail your comment or request, including your address and phone number to sherette.funncoleman@hhs.gov, or call the Reports Clearance Office on (202) 690–6162. Written comments and recommendations for the proposed information collections must be directed to the OS Paperwork Clearance Officer at the above e-mail address within 60 days.

A. Abstract

As a result of the Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA) (Pub. L. 111–5), the Office for Civil Rights (OCR) is required to revise its information collection under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules (45 CFR Parts 160 and 164). ARRA was enacted on February 17, 2009. This supporting statement revises a previously approved OCR data collection, OMB # 0990–0294. The HITECH Act requires modification of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub. L. 104–191) implementing regulations at 45 CFR Parts 160 and 164, the HIPAA Privacy and Security Rules, to extend jurisdiction to business associates and to strengthen privacy and

security protections for health information.

We have integrated this PRA notice into the Notice of Proposed Rulemaking, because these costs represent costs to be incurred as one-time, first year implementation costs. The estimated annualized burden table below was developed using the same estimates and workload assumptions in the impact statement in the section regarding Executive Order 12866, above. Because the HIPAA Privacy and Security Rules have been in effect for several years, these numbers, as revised pursuant to the HITECH modifications, are based on past experience with the current information collection.

With respect to the § 164.520 requirement to revise the Notice of Privacy Practices, the "Number of Respondents" column represents the number of covered entities that would be required to revise their Notices of Privacy Practices pursuant to the HITECH modifications. As such, 701,500 covered entities would be required to modify their Notices of Privacy Practices. Each covered entity would have to revise one Notice of Privacy Practices, which is represented by the "Average Number of Responses per Respondent" column. We estimate that each revision would require 20 minutes to complete. As such, it would take 233,833 total burden hours for 701,500 covered entities to revise their Notices of Privacy Practices. With respect to the § 164.520 requirement for health plans to disseminate the revised Notice of Privacy Practices, the "Number of Respondents" column represents the 200 million individuals to whom the revised Notice of Privacy Practices would be sent. Each individual would receive one Notice of Privacy Practices, which is represented by the "Average Number of Responses per Respondent" column. We estimate that each health plan would need one hour to prepare 100 Notices of Privacy Practices for mailing to individuals. As such, the total burden hours it would take health plans to disseminate Notices of Privacy Practices to 200 million individuals would be two million.

With regard to the proposed business associate provisions, as discussed in Section VI of this proposed rule, we assume that business associates currently comply with the HIPAA Privacy and Security Rules, and that their contracts range from the minimal compliance to avoid contract termination to being fully compliant. Because the proposed rule provides that most business associates may renegotiate their contracts during the compliance period in the normal course of business, we anticipate no or minimal additional burden. However, for those business associates with subcontractors, we anticipate an increased burden associated with bringing their subcontractors into compliance with the HIPAA Privacy and Security Rules, specifically with regard to business associate agreements.

Currently, business associates must obtain satisfactory assurance from their subcontractors regarding their compliance with the HIPAA Privacy and Security Rules. We assume that business associates obtained this satisfactory assurance via contract with their subcontractors. This proposed rule contains a new explicit requirement that business associates enter into contracts with their subcontractors to ensure compliance with the HIPAA Privacy and Security Rules. Because most business associates already have contracts in place, this new requirement creates a minimal additional burden associated with modification of these contracts. As discussed in Section VI above, we estimated that it will require one hour of a legal professional's time to modify these contracts. We estimate the number of business associates that may have to bring subcontractors into compliance to be 1,500,000. Our estimate is based on an average of one to two million business associates. This correlates to 1,500,000 burden hours.

The overall total for respondents to comply with the information collection requirements of the Rules is 3,733,833 burden hours. We request comment on this estimate.

As discussed in the above paragraph, we consider the majority of, if not all of, the burden associated with this proposed rule to result from the requirements with regard to the Notice of Privacy Practices and costs for business associates. However, as there may be an additional minimal burden associated with other provisions of the proposed rule, we request comment on the impacts of such provisions, as follows.

With regard to the proposed marketing, sale, fundraising, and access provisions discussed above in Section VI of this proposed rule, we do not anticipate any significant increase in the burden to covered entities and business associates, because covered entities already have in place routine business policies, procedures, and forms to address the current requirements regarding an opt-out for fundraising, authorizations for marketing and sale of protected health information, and the provision of access to electronic protected health information. While the proposed rule strengthens consumer protections in each of these areas, we do not have sufficient data on the current marketing, sale, fundraising, and access activities of covered entities and their business associates to calculate the impact of the increased protections on the use of these forms and processes.

B. Estimated Annualized Burden Table

Section	Type of respondent	Number of respondents	Average number of responses per respondent	Average burden hours per response	Total burden hours
164.504	Business Associates	1,500,000	1	1	1,500,000
164.520	Revision of Notice of Privacy Practices for Protected Health Information (drafting revised language).	701,500	1	20/60	233,833
164.520	Dissemination of Notice of Privacy Practices for Protected Health Information (health plans).	200,000,000	1	1 per 100	2,000,000
Total					3,733,833

List of Subjects

45 CFR Part 160

Administrative practice and procedure, Computer technology, Electronic information system, Electronic transactions, Employer benefit plan, Health, Health care, Health facilities, Health insurance, Health records, Hospitals, Investigations, Medicaid, Medical research, Medicare, Penalties, Privacy, Reporting and record keeping requirements, Security.

45 CFR Part 164

Administrative practice and procedure, Computer technology, Electronic information system, Electronic transactions, Employer benefit plan, Health, Health care, Health facilities, Health insurance, Health records, Hospitals, Medicaid, Medical research, Medicare, Privacy, Reporting and record keeping requirements, Security.

For the reasons set forth in the preamble, the Department proposes to amend 45 CFR Subtitle A, Subchapter C, parts 160 and 164, as set forth below:

PART 160—GENERAL ADMINISTRATIVE REQUIREMENTS

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

Authority: 42 U.S.C. 1302(a); 42 U.S.C. 1320d–1320d–8; sec. 264, Pub. L. 104–191, 110 Stat. 2033–2034 (42 U.S.C. 1320d–2(note)); 5 U.S.C. 552; and secs. 13400–13424, Pub. L. 111–5, 123 Stat. 258–279.

2. Revise § 160.101 to read as follows:

§ 160.101 Statutory basis and purpose.

The requirements of this subchapter implement sections 1171–1179 of the Social Security Act (the Act), as added by section 262 of Public Law 104–191, section 264 of Public Law 104–191, and sections 13400–13424 of Public Law 111–5.

3. Amend § 160.102 as follows:

a. Redesignate paragraph (b) as paragraph (c); and

b. Add new paragraph (b) to read as follows:

§ 160.102 Applicability.

* * * * *

(b) Where provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to a business associate.

* * * * *

4. Amend § 160.103 as follows:

a. Revise the definitions of "business associate", "compliance date", "disclosure", "electronic media", paragraph (2) of "protected health information," and the definitions of "standard", "State", and "workforce"; and

b. Add, in alphabetical order, new definitions of "administrative simplification provision", "ALJ", "civil money penalty or penalty", "respondent", "subcontractor", and "violation or violate".

The revisions and additions read as follows:

§ 160.103 Definitions.

* * * * *

Administrative simplification provision means any requirement or prohibition established by:

(1) 42 U.S.C. 1320d–1320d–4, 1320d–7, and 1320d–8;

(2) Section 264 of Pub. L. 104–191;

(3) Sections 13400–13424 of Public Law 111–5; or

(4) This subchapter.

ALJ means Administrative Law Judge.

* * * * *

Business associate: (1) Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:

(A) A function or activity involving the use or disclosure of protected health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or

(B) Any other function or activity regulated by this subchapter; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity may be a business associate of another covered entity.

(3) *Business associate* includes:

(i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.

(ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.

(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

(4) *Business associate* does not include:

(i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

(ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of this subchapter apply and are met.

(iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.

(iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services.

Civil money penalty or *penalty* means the amount determined under § 160.404 of this part and includes the plural of these terms.

* * * * *

Compliance date means the date by which a covered entity or business associate must comply with a standard, implementation specification, requirement, or modification adopted under this subchapter.

* * * * *

Disclosure means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.

* * * * *

Electronic media means:

(1) Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card;

(2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet (wide-open), extranet or intranet (using Internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-

up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form before the transmission.

* * * * *

Protected health information * * *

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

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

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

(iii) In employment records held by a covered entity in its role as employer; and

(iv) Regarding a person who has been deceased for more than 50 years.

* * * * *

Respondent means a covered entity or business associate upon which the Secretary has imposed, or proposes to impose, a civil money penalty.

* * * * *

Standard means a rule, condition, or requirement:

(1) Describing the following information for products, systems, services, or practices:

(i) Classification of components;

(ii) Specification of materials, performance, or operations; or

(iii) Delineation of procedures; or

(2) With respect to the privacy of protected health information.

* * * * *

State refers to one of the following:

(1) For a health plan established or regulated by Federal law, State has the meaning set forth in the applicable section of the United States Code for such health plan.

(2) For all other purposes, *State* means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.

Subcontractor means a person who acts on behalf of a business associate, other than in the capacity of a member of the workforce of such business associate.

* * * * *

Violation or *violate* means, as the context may require, failure to comply with an administrative simplification provision.

Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.

5. Add § 160.105 to subpart A to read as follows:

§ 160.105 Compliance dates for implementation of new or modified standards and implementation specifications.

In accordance with § 160.104, with respect to new standards and implementation specifications or modifications to standards and implementation specifications in this subchapter that become effective after [DATE OF PUBLICATION OF THE FINAL RULE IN THE FEDERAL REGISTER], except as otherwise provided, covered entities and business associates must comply with the applicable new standards and implementation specifications or modifications to standards and implementation specifications no later than 180 days from the effective date of any such standards or implementation specifications.

6. Revise § 160.201 to read as follows:

§ 160.201 Statutory basis.

The provisions of this subpart implement section 1178 of the Act, as added by section 262 of Public Law 104–191, section 264(c) of Public Law 104–191, and section 13421(a) of Public Law 111–5.

7. In § 160.202, revise the definition of "contrary" and paragraph (1)(i) of the definition of "more stringent" to read as follows:

§ 160.202 Definitions.

* * * * *

Contrary, when used to compare a provision of State law to a standard, requirement, or implementation specification adopted under this subchapter, means:

(1) A covered entity or business associate would find it impossible to comply with both the State and Federal requirements; or

(2) The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act, section 264 of Public Law 104–191, or sections 13400–13424 of Public Law 111–5, as applicable.

More stringent * * *

(1) * * *

(i) Required by the Secretary in connection with determining whether a covered entity or business associate is in compliance with this subchapter; or

* * * * *

8. Revise § 160.300 to read as follows:

§ 160.300 Applicability.

This subpart applies to actions by the Secretary, covered entities, business associates, and others with respect to ascertaining the compliance by covered entities and business associates with, and the enforcement of, the applicable provisions of this part 160 and parts 162 and 164 of this subchapter.

§ 160.302 [Removed and Reserved]

9. Remove and reserve § 160.302.

10. Revise § 160.304 to read as follows:

§ 160.304 Principles for achieving compliance.

(a) *Cooperation.* The Secretary will, to the extent practicable and consistent with the provisions of this subpart, seek the cooperation of covered entities and business associates in obtaining compliance with the applicable administrative simplification provisions.

(b) *Assistance.* The Secretary may provide technical assistance to covered entities and business associates to help them comply voluntarily with the applicable administrative simplification provisions.

11. In § 160.306, revise paragraphs (a) and (c) to read as follows:

§ 160.306 Complaints to the Secretary.

(a) *Right to file a complaint.* A person who believes a covered entity or business associate is not complying with the administrative simplification provisions may file a complaint with the Secretary.

* * * * *

(c) *Investigation.*

(1) The Secretary will investigate any complaint filed under this section when a preliminary review of the facts indicates a possible violation due to willful neglect.

(2) The Secretary may investigate any other complaint filed under this section.

(3) An investigation under this section may include a review of the pertinent policies, procedures, or practices of the covered entity or business associate and of the circumstances regarding any alleged violation.

(4) At the time of the initial written communication with the covered entity or business associate about the complaint, the Secretary will describe the acts and/or omissions that are the basis of the complaint.

12. Revise § 160.308 to read as follows:

§ 160.308 Compliance reviews.

(a) The Secretary will conduct a compliance review to determine whether a covered entity or business associate is complying with the applicable administrative simplification provisions when a preliminary review of the facts indicates a possible violation due to willful neglect.

(b) The Secretary may conduct a compliance review to determine whether a covered entity or business associate is complying with the applicable administrative simplification provisions in any other circumstance.

13. Revise § 160.310 to read as follows:

§ 160.310 Responsibilities of covered entities and business associates.

(a) *Provide records and compliance reports.* A covered entity or business associate must keep such records and submit such compliance reports, in such time and manner and containing such information, as the Secretary may determine to be necessary to enable the Secretary to ascertain whether the covered entity or business associate has complied or is complying with the applicable administrative simplification provisions.

(b) *Cooperate with complaint investigations and compliance reviews.* A covered entity or business associate must cooperate with the Secretary, if the Secretary undertakes an investigation or compliance review of the policies, procedures, or practices of the covered entity or business associate to determine whether it is complying with the applicable administrative simplification provisions.

(c) *Permit access to information.*

(1) A covered entity or business associate must permit access by the Secretary during normal business hours to its facilities, books, records, accounts, and other sources of information, including protected health information, that are pertinent to ascertaining compliance with the applicable administrative simplification provisions. If the Secretary determines that exigent circumstances exist, such as when documents may be hidden or destroyed, a covered entity or business associate must permit access by the Secretary at any time and without notice.

(2) If any information required of a covered entity or business associate under this section is in the exclusive possession of any other agency, institution, or person and the other agency, institution, or person fails or refuses to furnish the information, the covered entity or business associate must so certify and set forth what efforts it has made to obtain the information.

(3) Protected health information obtained by the Secretary in connection with an investigation or compliance review under this subpart will not be disclosed by the Secretary, except if necessary for ascertaining or enforcing compliance with the applicable administrative simplification provisions, if otherwise required by law, or if permitted under 5 U.S.C. 552a(b)(7).

14. Revise § 160.312 to read as follows:

§ 160.312 Secretarial action regarding complaints and compliance reviews.

(a) *Resolution when noncompliance is indicated.*

(1) If an investigation of a complaint pursuant to § 160.306 or a compliance review pursuant to § 160.308 indicates noncompliance, the Secretary may attempt to reach a resolution of the matter satisfactory to the Secretary by informal means. Informal means may include demonstrated compliance or a completed corrective action plan or other agreement.

(2) If the matter is resolved by informal means, the Secretary will so inform the covered entity or business associate and, if the matter arose from a complaint, the complainant, in writing.

(3) If the matter is not resolved by informal means, the Secretary will—

(i) So inform the covered entity or business associate and provide the covered entity or business associate an opportunity to submit written evidence of any mitigating factors or affirmative defenses for consideration under §§ 160.408 and 160.410 of this part. The covered entity or business associate must submit any such evidence to the Secretary within 30 days (computed in the same manner as prescribed under § 160.526 of this part) of receipt of such notification; and

(ii) If, following action pursuant to paragraph (a)(3)(i) of this section, the Secretary finds that a civil money penalty should be imposed, inform the covered entity or business associate of such finding in a notice of proposed determination in accordance with § 160.420 of this part.

(b) *Resolution when no violation is found.* If, after an investigation pursuant to § 160.306 or a compliance review pursuant to § 160.308, the Secretary determines that further action is not warranted, the Secretary will so inform the covered entity or business associate and, if the matter arose from a complaint, the complainant, in writing.

15. In § 160.316, revise the introductory text to read as follows:

§ 160.316 Refraining from intimidation or retaliation.

A covered entity or business associate may not threaten, intimidate, coerce, harass, discriminate against, or take any other retaliatory action against any individual or other person for—

* * * * *

16. In § 160.401, revise the definition of *reasonable cause* to read as follows:

§ 160.401 Definitions.

* * * * *

Reasonable cause means an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect.

* * * * *

17. Revise § 160.402 to read as follows:

§ 160.402 Basis for a civil money penalty.

(a) *General rule.* Subject to § 160.410, the Secretary will impose a civil money penalty upon a covered entity or business associate if the Secretary determines that the covered entity or business associate has violated an administrative simplification provision.

(b) *Violation by more than one covered entity or business associate.*

(1) Except as provided in paragraph (b)(2) of this section, if the Secretary determines that more than one covered entity or business associate was responsible for a violation, the Secretary will impose a civil money penalty against each such covered entity or business associate.

(2) A covered entity that is a member of an affiliated covered entity, in accordance with § 164.105(b) of this subchapter, is jointly and severally liable for a civil money penalty for a violation of part 164 of this subchapter based on an act or omission of the affiliated covered entity, unless it is established that another member of the affiliated covered entity was responsible for the violation.

(c) *Violation attributed to a covered entity or business associate.* (1) A covered entity is liable, in accordance with the Federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the covered entity, including a workforce member or business associate, acting within the scope of the agency.

(2) A business associate is liable, in accordance with the Federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the business associate, including a workforce member or subcontractor, acting within the scope of the agency.

18. In § 160.404, revise the introductory text of paragraphs (b)(2)(i), (b)(2)(iii), and (b)(2)(iv) to read as follows:

§ 160.404 Amount of a civil money penalty.

* * * * *

(b) * * *

(2) * * *

(i) For a violation in which it is established that the covered entity or business associate did not know and, by exercising reasonable diligence, would not have known that the covered entity or business associate violated such provision,

* * * * *

(iii) For a violation in which it is established that the violation was due to willful neglect and was corrected during the 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred,

* * * * *

(iv) For a violation in which it is established that the violation was due to willful neglect and was not corrected during the 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred,

* * * * *

19. Revise § 160.406 to read as follows:

§ 160.406 Violations of an identical requirement or prohibition.

The Secretary will determine the number of violations of an administrative simplification provision based on the nature of the covered entity's or business associate's obligation to act or not act under the provision that is violated, such as its obligation to act in a certain manner, or within a certain time, or to act or not act with respect to certain persons. In the case of continuing violation of a provision, a separate violation occurs each day the covered entity or business associate is in violation of the provision.

20. Revise § 160.408 to read as follows:

§ 160.408 Factors considered in determining the amount of a civil money penalty.

In determining the amount of any civil money penalty, the Secretary will consider the following factors, which may be mitigating or aggravating as appropriate:

(a) The nature and extent of the violation, consideration of which may include but is not limited to:

(1) The number of individuals affected; and

(2) The time period during which the violation occurred;

(b) The nature and extent of the harm resulting from the violation, consideration of which may include but is not limited to:

(1) Whether the violation caused physical harm;

(2) Whether the violation resulted in financial harm;

(3) Whether the violation resulted in harm to an individual's reputation; and

(4) Whether the violation hindered an individual's ability to obtain health care;

(c) The history of prior compliance with the administrative simplification provisions, including violations, by the covered entity or business associate, consideration of which may include but is not limited to:

(1) Whether the current violation is the same or similar to previous indications of noncompliance;

(2) Whether and to what extent the covered entity or business associate has attempted to correct previous indications of noncompliance;

(3) How the covered entity or business associate has responded to technical assistance from the Secretary provided in the context of a compliance effort; and

(4) How the covered entity or business associate has responded to prior complaints;

(d) The financial condition of the covered entity or business associate, consideration of which may include but is not limited to:

(1) Whether the covered entity or business associate had financial difficulties that affected its ability to comply;

(2) Whether the imposition of a civil money penalty would jeopardize the ability of the covered entity or business associate to continue to provide, or to pay for, health care; and

(3) The size of the covered entity or business associate; and

(e) Such other matters as justice may require.

21. Revise § 160.410 to read as follows:

§ 160.410 Affirmative defenses.

(a) The Secretary may not:

(1) Prior to February 18, 2011, impose a civil money penalty on a covered entity or business associate for an act that violates an administrative simplification provision if the covered entity or business associate establishes that the violation is punishable under 42 U.S.C. 1320d–6.

(2) On or after February 18, 2011, impose a civil money penalty on a covered entity or business associate for an act that violates an administrative simplification provision if the covered entity or business associate establishes that a penalty has been imposed under 42 U.S.C. 1320d-6 with respect to such act.

(b) For violations occurring prior to February 18, 2009, the Secretary may not impose a civil money penalty on a covered entity for a violation if the covered entity establishes that an affirmative defense exists with respect to the violation, including the following:

(1) The covered entity establishes, to the satisfaction of the Secretary, that it did not have knowledge of the violation, determined in accordance with the Federal common law of agency, and by exercising reasonable diligence, would not have known that the violation occurred; or

(2) The violation is—

(i) Due to circumstances that would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated and is not due to willful neglect; and

(ii) Corrected during either:

(A) The 30-day period beginning on the first date the covered entity liable for the penalty knew, or by exercising reasonable diligence would have known, that the violation occurred; or

(B) Such additional period as the Secretary determines to be appropriate based on the nature and extent of the failure to comply.

(c) For violations occurring on or after February 18, 2009, the Secretary may not impose a civil money penalty on a covered entity or business associate for a violation if the covered entity or business associate establishes to the satisfaction of the Secretary that the violation is—

(1) Not due to willful neglect; and

(2) Corrected during either:

(i) The 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred; or

(ii) Such additional period as the Secretary determines to be appropriate based on the nature and extent of the failure to comply.

22. Revise § 160.412 to read as follows:

§ 160.412 Waiver.

For violations described in § 160.410(b)(2) or (c) that are not corrected within the period specified under such paragraphs, the Secretary may waive the civil money penalty, in whole or in part, to the extent that the payment of the penalty would be excessive relative to the violation.

23. Revise § 160.418 to read as follows:

§ 160.418 Penalty not exclusive.

Except as otherwise provided by 42 U.S.C. 1320d–5(b)(1) and 42 U.S.C. 299b–22(f)(3), a penalty imposed under this part is in addition to any other penalty prescribed by law.

PART 164—SECURITY AND PRIVACY

24. The authority citation for part 164 is revised to read as follows:

Authority: 42 U.S.C. 1302(a); 42 U.S.C. 1320d—1320d–8; sec. 264, Pub. L. 104–191, 110 Stat. 2033–2034 (42 U.S.C. 1320–2(note)); and secs. 13400—13424, Pub. L. 111–5, 123 Stat. 258–279.

25. Revise § 164.102 to read as follows:

§ 164.102 Statutory basis.

The provisions of this part are adopted pursuant to the Secretary's authority to prescribe standards, requirements, and implementation specifications under part C of title XI of the Act, section 264 of Public Law 104–191, and sections 13400—13424 of Public Law 111–5.

26. In § 164.104, revise paragraph (b) to read as follows:

§ 164.104 Applicability.

* * * * *

(b) Where provided, the standards, requirements, and implementation specifications adopted under this part apply to a business associate.

27. Amend § 164.105 as follows:

a. Revise the introductory text of paragraph (a)(1), the introductory text of paragraph (a)(2)(i), paragraph (a)(2)(ii), the introductory text of paragraph (a)(2)(iii), and paragraphs (a)(2)(iii)(A) and (B);

b. Redesignate paragraph (a)(2)(iii)(C) as paragraph (a)(2)(iii)(D) and add new paragraph (a)(2)(iii)(C); and

c. Revise paragraph (b).

The revisions read as follows:

§ 164.105 Organizational requirements.

(a)(1) *Standard: Health care component.* If a covered entity is a hybrid entity, the requirements of this part, other than the requirements of this section, § 164.314, and § 164.504, apply only to the health care component(s) of the entity, as specified in this section.

(2) * * *

(i) *Application of other provisions.* In applying a provision of this part, other than the requirements of this section, § 164.314, and § 164.504, to a hybrid entity:

* * * * *

(ii) *Safeguard requirements.* The covered entity that is a hybrid entity must ensure that a health care component of the entity complies with the applicable requirements of this part. In particular, and without limiting this requirement, such covered entity must ensure that:

(A) Its health care component does not disclose protected health information to another component of the covered entity in circumstances in which subpart E of this part would prohibit such disclosure if the health care component and the other component were separate and distinct legal entities;

(B) Its health care component protects electronic protected health information with respect to another component of the covered entity to the same extent that it would be required under subpart C of this part to protect such information if the health care component and the other component were separate and distinct legal entities;

(C) If a person performs duties for both the health care component in the capacity of a member of the workforce of such component and for another component of the entity in the same capacity with respect to that component, such workforce member must not use or disclose protected health information created or received in the course of or incident to the member's work for the health care component in a way prohibited by subpart E of this part.

(iii) *Responsibilities of the covered entity.* A covered entity that is a hybrid entity has the following responsibilities:

(A) For purposes of subpart C of part 160 of this subchapter, pertaining to compliance and enforcement, the covered entity has the responsibility of complying with this part.

(B) The covered entity is responsible for complying with § 164.316(a) and § 164.530(i), pertaining to the implementation of policies and procedures to ensure compliance with applicable requirements of this part, including the safeguard requirements in paragraph (a)(2)(ii) of this section.

(C) The covered entity is responsible for complying with § 164.314 and § 164.504 regarding business associate arrangements and other organizational requirements.

* * * * *

(b)(1) *Standard: Affiliated covered entities.* Legally separate covered entities that are affiliated may designate themselves as a single covered entity for purposes of this part.

(2) *Implementation specifications.*

(i) *Requirements for designation of an affiliated covered entity.* (A) Legally separate covered entities may designate themselves (including any health care component of such covered entity) as a single affiliated covered entity, for purposes of this part, if all of the covered entities designated are under common ownership or control.

(B) The designation of an affiliated covered entity must be documented and the documentation maintained as required by paragraph (c) of this section.

(ii) *Safeguard requirements.* An affiliated covered entity must ensure that it complies with the applicable requirements of this part, including, if the affiliated covered entity combines the functions of a health plan, health care provider, or health care clearinghouse, § 164.308(a)(4)(ii)(A) and § 164.504(g), as applicable.

* * * * *

28. Revise § 164.106 to read as follows:

§ 164.106 Relationship to other parts.

In complying with the requirements of this part, covered entities and, where provided, business associates, are required to comply with the applicable provisions of parts 160 and 162 of this subchapter.

29. The authority citation for subpart C of part 164 is revised to read as follows:

Authority: 42 U.S.C. 1320d–2 and 1320d–4; sec. 13401, Pub. L. 111–5, 123 Stat. 260.

30. Revise § 164.302 to read as follows:

§ 164.302 Applicability.

A covered entity or business associate must comply with the applicable standards, implementation specifications, and requirements of this subpart with respect to electronic protected health information of a covered entity.

31. In § 164.304, revise the definitions of *Administrative safeguards* and *Physical safeguards* to read as follows:

§ 164.304 Definitions.

* * * * *

Administrative safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.

* * * * *

Physical safeguards are physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

* * * * *

32. Amend § 164.306 as follows:

a. Revise the introductory text of paragraph (a) and paragraph (a)(1);

b. Revise paragraph (b)(1), the introductory text of paragraph (b)(2), and paragraphs (b)(2)(i) and (b)(2)(ii);

c. Revise paragraph (c);

d. Revise paragraph (d)(2), the introductory text of paragraph (d)(3), paragraph (d)(3)(i), and the introductory text of paragraph (d)(3)(ii); and

e. Revise paragraph (e).

The revisions read as follows:

§ 164.306 Security standards: General rules.

(a) *General requirements.* Covered entities and business associates must do the following:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.

* * * * *

(b) * * * (1) Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.

(2) In deciding which security measures to use, a covered entity or business associate must take into account the following factors:

(i) The size, complexity, and capabilities of the covered entity or business associate.

(ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities.

* * * * *

(c) *Standards.* A covered entity or business associate must comply with the applicable standards as provided in this section and in § 164.308, § 164.310, § 164.312, § 164.314 and § 164.316 with respect to all electronic protected health information.

(d) * * *

(2) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes required implementation specifications, a covered entity or business associate must implement the implementation specifications.

(3) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes addressable implementation specifications, a covered entity or business associate must—

(i) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting electronic protected health information; and

(ii) As applicable to the covered entity or business associate—

* * * * *

(e) *Maintenance.* A covered entity or business associate must review and modify the security measures implemented under this subpart as needed to continue provision of reasonable and appropriate protection of electronic protected health information, and update documentation of such security measures in accordance with § 164.316(b)(2)(iii).

33. Amend § 164.308 as follows:

a. Revise the introductory text of paragraph (a), paragraph (a)(1)(ii)(A), paragraph (a)(1)(ii)(C), paragraph (a)(2), paragraph (a)(3)(ii)(C), paragraph (a)(4)(ii)(C), paragraph (a)(6)(ii), and paragraph (a)(8); and

b. Revise paragraph (b).

The revisions read as follows:

§ 164.308 Administrative safeguards.

(a) A covered entity or business associate must, in accordance with § 164.306:

(1) * * *

(ii) * * *

(A) *Risk analysis (Required).* Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

* * * * *

(C) *Sanction policy (Required).* Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

* * * * *

(2) *Standard: Assigned security responsibility.* Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.

(3) * * *

(ii) * * *

(C) *Termination procedures* (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

(4) * * *

(ii) * * *

(C) *Access establishment and modification* (Addressable). Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

* * * * *

(6) * * *

(ii) *Implementation specification: Response and reporting* (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

* * * * *

(8) *Standard: Evaluation.* Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.

(b)(1) *Business associate contracts and other arrangements.* A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

(2) A business associate may permit a business associate that is a

subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information.

(3) *Implementation specifications: Written contract or other arrangement* (Required). Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).

34. Revise the introductory text of § 164.310 to read as follows:

§ 164.310 Physical safeguards.

A covered entity or business associate must, in accordance with § 164.306:

* * * * *

35. Revise the introductory text of § 164.312 to read as follows:

§ 164.312 Technical safeguards.

A covered entity or business associate must, in accordance with § 164.306:

* * * * *

36. Amend § 164.314 by revising paragraphs (a) and (b)(2)(iii) to read as follows:

§ 164.314 Organizational requirements.

(a)(1) *Standard: Business associate contracts or other arrangements.* The contract or other arrangement required by § 164.308(b)(4) must meet the requirements of paragraph (a)(2)(i), (a)(2)(ii), or (a)(2)(iii) of this section, as applicable.

(2) *Implementation specifications* (Required).

(i) *Business associate contracts.* The contract must provide that the business associate will—

(A) Comply with the applicable requirements of this subpart;

(B) In accordance with § 164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section; and

(C) Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410.

(ii) *Other arrangements.* The covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of § 164.504(e)(3).

(iii) *Business associate contracts with subcontractors.* The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by § 164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.

(b) * * *

(2) * * *

(iii) Ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and

* * * * *

37. Revise the introductory text of § 164.316 and the third sentence of paragraph (a) to read as follows:

§ 164.316 Policies and procedures and documentation requirements.

A covered entity or business associate must, in accordance with § 164.306:

(a) * * * A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.

* * * * *

38. The authority citation for subpart E of part 164 is revised to read as follows:

Authority: 42 U.S.C. 1320d–2 and 1320d–4; sec. 264 of Pub. L. 104–191, 110 Stat. 2033–2034 (42 U.S.C. 1320d–2 (note)); and secs. 13400–13424, Pub. L. 111–5, 123 Stat. 258–279.

39. In § 164.500, redesignate paragraph (c) as paragraph (d) and add new paragraph (c) to read as follows:

§ 164.500 Applicability.

* * * * *

(c) Where provided, the standards, requirements, and implementation specifications adopted under this subpart apply to a business associate with respect to the protected health information of a covered entity.

* * * * *

40. Amend § 164.501 as follows:

a. Revise paragraph (1) of the definition of "health care operations"; and

b. Revise the definition of "marketing".

The revisions read as follows:

§ 164.501 Definitions.

* * * * *

Health care operations * * *

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

* * * * *

Marketing: (1) Except as provided in paragraph (2) of this definition, marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

(2) Marketing does not include a communication made:

(i) For treatment of an individual by a health care provider, including 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, provided, however, that if the communication is in writing and the health care provider receives financial remuneration in exchange for making the communication, the requirements of § 164.514(f)(2) are met.

(ii) To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity's cost of making the communication.

(iii) For the following health care operations activities, except where the covered entity receives financial remuneration in exchange for making the communication:

(A) 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; or

(B) For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

(3) *Financial remuneration* means direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual.

* * * * *

41. In § 164.502, revise paragraphs (a), (b)(1), (e), and (f) to read as follows:

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

(a) *Standard.* A covered entity or business associate may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

(1) *Covered entities: Permitted uses and disclosures.* A covered entity is permitted to use or disclose protected health information as follows:

(i) To the individual;

(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;

(iv) Pursuant to and in compliance with a valid authorization under § 164.508;

(v) Pursuant to an agreement under, or as otherwise permitted by, § 164.510; and

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

(2) *Covered entities: Required disclosures.* A covered entity is required to disclose protected health information:

(i) To an individual, when requested under, and required by § 164.524 or § 164.528; and

(ii) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subchapter.

(3) [*Reserved]*

(4) *Business associates: Permitted uses and disclosures.* (i) A business associate may use or disclose protected health information only as permitted or required by its business associate contract or other arrangement pursuant to § 164.504(e), or as required by law. The business associate may not use or disclose protected health information in a manner that would violate the requirements of this subpart, if done by the covered entity, except for the purposes specified under § 164.504(e)(2)(i)(A) or (B) if such uses or disclosures are permitted by its contract or other arrangement.

(5) *Business associates: Required uses and disclosures.* A business associate is required to disclose protected health information:

(i) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the business associate's compliance with this subchapter.

(ii) To the covered entity, individual, or individual's designee, as necessary to satisfy a covered entity's obligations under § 164.524(c)(2)(ii) and (3)(ii) with respect to an individual's request for an electronic copy of protected health information.

(b) * * * (1) *Minimum necessary applies.* When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

* * * * *

(e)(1) *Standard: Disclosures to business associates.* (i) A covered entity may disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

(ii) A business associate may disclose protected health information to a business associate that is a subcontractor and may allow the subcontractor to create or receive protected health information on its behalf, if the business associate obtains satisfactory assurances, in accordance with § 164.504(e)(1)(i), that the subcontractor will appropriately safeguard the information.

(2) *Implementation specification: Documentation.* The satisfactory assurances required by paragraph (e)(1) of this section must be documented through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of § 164.504(e).

(f) *Standard: Deceased individuals.* A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual for a period of 50 years following the death of the individual.

* * * * *

42. In § 164.504, revise paragraphs (e) and (f)(2)(ii)(B) to read as follows:

§ 164.504 Uses and disclosures: Organizational requirements.

* * * * *

(e)(1) *Standard: Business associate contracts.* (i) The contract or other arrangement required by § 164.502(e)(2) must meet the requirements of paragraph (e)(2), (e)(3), or (e)(5) of this section, as applicable.

(ii) A covered entity is not in compliance with the standards in § 164.502(e) and this paragraph, if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

(iii) A business associate is not in compliance with the standards in § 164.502(e) and this paragraph, if the business associate knew of a pattern of activity or practice of a subcontractor that constituted a material breach or violation of the subcontractor's obligation under the contract or other arrangement, unless the business associate took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

(2) *Implementation specifications: Business associate contracts.* A contract between the covered entity and a business associate must:

(i) Establish the permitted and required uses and disclosures of protected health information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity, except that:

(A) The contract may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate, as provided in paragraph (e)(4) of this section; and

(B) The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.

(ii) Provide that the business associate will:

(A) Not use or further disclose the information other than as permitted or required by the contract or as required by law;

(B) Use appropriate safeguards and comply, where applicable, with subpart C of this part with respect to electronic protected health information, to prevent use or disclosure of the information other than as provided for by its contract;

(C) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410;

(D) In accordance with § 164.502(e)(1)(ii), ensure that any subcontractors that create or receive protected health information on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information;

(E) Make available protected health information in accordance with § 164.524;

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with § 164.526;

(G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528;

(H) To the extent the business associate is to carry out a covered entity's obligation under this subpart, comply with the requirements of this subpart that apply to the covered entity in the performance of such obligation.

(I) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and

(J) At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

(iii) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

(3) *Implementation specifications: Other arrangements.* (i) If a covered entity and its business associate are both governmental entities:

(A) The covered entity may comply with this paragraph and § 164.314(a)(1), if applicable, by entering into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (e)(2) of this section and § 164.314(a)(2), if applicable.

(B) The covered entity may comply with this paragraph and § 164.314(a)(1), if applicable, if other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (e)(2) of this section and § 164.314(a)(2), if applicable.

(ii) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of *business associate* in § 160.103 of this subchapter to a covered entity, such covered entity may disclose protected health information to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements of this paragraph and § 164.314(a)(1), if applicable, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (e)(2) of this section and § 164.314(a)(1), if applicable, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained.

(iii) The covered entity may omit from its other arrangements the termination authorization required by paragraph (e)(2)(iii) of this section, if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.

(4) *Implementation specifications: Other requirements for contracts and other arrangements.* (i) The contract or other arrangement between the covered entity and the business associate may permit the business associate to use the protected health information received by the business associate in its capacity as a business associate to the covered entity, if necessary:

(A) For the proper management and administration of the business associate; or

(B) To carry out the legal responsibilities of the business associate.

(ii) The contract or other arrangement between the covered entity and the business associate may permit the business associate to disclose the protected health information received by the business associate in its capacity as a business associate for the purposes described in paragraph (e)(4)(i) of this section, if:

(A) The disclosure is required by law; or

(B)(*1*) The business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person; and

(*2*) The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(5) *Implementation specifications: Business associate contracts with subcontractors.* The requirements of § 164.504(e)(2) through (e)(4) apply to the contract or other arrangement required by § 164.502(e)(1)(ii) between a business associate and a business associate that is a subcontractor in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.

(f) * * *

(2) * * *

(ii) * * *

(B) Ensure that any agents to whom it provides protected health information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;

* * * * *

43. Revise § 164.506(c)(5) to read as follows:

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

* * * * *

(c) * * *

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

44. Amend § 164.508 as follows:

a. Revise the headings of paragraphs (a), (a)(1), and (a)(2);

b. Revise paragraph (a)(3)(ii);

c. Add new paragraph (a)(4); and

d. Revise paragraphs (b)(1)(i), and (b)(3).

The revisions and additions 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.* * * *

(2) *Authorization required: Psychotherapy notes.* * * *

(3) * * *

(ii) If the marketing involves direct or indirect financial remuneration, as defined in paragraph (3) of the definition of marketing at § 164.501, to the covered entity from a third party, the authorization must state that such remuneration is involved.

(4) *Authorization required: Sale of protected health information.* (i) Notwithstanding any provision of this subpart, a covered entity must obtain an authorization for any disclosure of protected health information for which the disclosure is in exchange for direct or indirect remuneration from or on behalf of the recipient of the protected health information. Such authorization must state that the disclosure will result in remuneration to the covered entity.

(ii) Paragraph (a)(4)(i) of this section does not apply to disclosures of protected health information:

(A) For public health purposes pursuant to § 164.512(b) or § 164.514(e);

(B) For research purposes pursuant to § 164.512(i) or § 164.514(e), where the only remuneration received by the covered entity is a reasonable cost-based fee to cover the cost to prepare and transmit the protected health information for such purposes;

(C) For treatment and payment purposes pursuant to § 164.506(a);

(D) For the sale, transfer, merger, or consolidation of all or part of the covered entity and for related due diligence as described in paragraph (6)(iv) of the definition of health care operations and pursuant to § 164.506(a);

(E) To or by a business associate for activities that the business associate undertakes on behalf of a covered entity pursuant to §§ 164.502(e) and 164.504(e), and the only remuneration provided is by the covered entity to the business associate for the performance of such activities;

(F) To an individual, when requested under § 164.524 or § 164.528;

(G) Required by law as permitted under § 164.512(a); and

(H) Permitted by and in accordance with the applicable requirements of this subpart, where the only remuneration received by the covered entity is a reasonable, cost-based fee to cover the cost to prepare and transmit the protected health information for such purpose or a fee otherwise expressly permitted by other law.

(b) * * *

(1) * * *

(i) A valid authorization is a document that meets the requirements in paragraphs (a)(3)(ii), (a)(4)(i), (c)(1), and (c)(2) of this section, as applicable.

* * * * *

(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 or another research study. This exception includes combining an authorization for the use or disclosure of protected health information for a research study with another authorization for the same research study, with an authorization for the creation or maintenance of a research database or repository, or with a consent to participate in research. Where a covered health care provider has conditioned the provision of research-related treatment on the provision of one of the authorizations, as permitted under paragraph (b)(4)(i) of this section, any compound authorization created under this paragraph must clearly differentiate between the conditioned and unconditioned components and provide the individual with an opportunity to opt in to the research activities described in the unconditioned authorization.

(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. The prohibition in this paragraph on combining authorizations where one authorization conditions the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits under paragraph (b)(4) of this section does not apply to a compound authorization created in accordance with paragraph (b)(3)(i) of this section.

* * * * *

45. Amend § 164.510 as follows:

a. Revise paragraph (a)(1)(ii) introductory text;

b. Revise paragraph (b)(1)(i), the second sentence of paragraph (b)(1)(ii), paragraph (b)(2)(iii), the first sentence of paragraph (b)(3), and paragraph (b)(4); and

c. Add new paragraph (b)(5).

The revisions and additions read as follows:

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

* * * * *

(a) * * *

(1) * * *

(ii) Use or disclose for directory purposes such information:

* * * * *

(b) * * *

(1) * * *

(i) A covered entity may, in accordance with paragraphs (b)(2), (b)(3), or (b)(5) of this section, disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the protected health information directly relevant to such person's involvement with the individual's health care or payment related to the individual's health care.

(ii) * * * Any such use or disclosure of protected health information for such notification purposes must be in accordance with paragraphs (b)(2), (b)(3), (b)(4), or (b)(5) of this section, as applicable.

* * * * *

(2) * * *

(iii) Reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure.

(3) * * * If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's care or payment related to the individual's health care or needed for notification purposes. * * *

(4) *Uses and disclosures for disaster relief purposes.* A covered entity may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures

permitted by paragraph (b)(1)(ii) of this section. The requirements in paragraphs (b)(2), (b)(3), or (b)(5) of this section apply to such uses and disclosures to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

(5) *Uses and disclosures when the individual is deceased.* If the individual is deceased, a covered entity may disclose protected health information of the individual to a family member, or other persons identified in paragraph (b)(1) of this section who were involved in the individual's care or payment for health care prior to the individual's death, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity.

46. Amend § 164.512 as follows:

a. Revise the introductory text of paragraph (b)(1) and the introductory text of paragraph (b)(1)(v)(A);

b. Add new paragraph (b)(1)(vi);

c. Revise the introductory text of paragraph (e)(1)(iii) and paragraph (e)(1)(vi);

d. Revise paragraph (i)(2)(iii); and

e. Revise paragraphs (k)(1)(ii), (k)(3), and (k)(5)(i)(E).

The revisions and additions read as follows:

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

* * * * *

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

(1) *Permitted uses and disclosures.* A covered entity may use or disclose protected health information for the public health activities and purposes described in this paragraph to:

* * * * *

(v) * * *

(A) The covered entity is a covered health care provider who provides health care to the individual at the request of the employer:

* * * * *

(vi) A school, about an individual who is a student or prospective student of the school, if:

(A) The protected health information that is disclosed is limited to proof of immunization;

(B) The school is required by State or other law to have such proof of immunization prior to admitting the individual; and

(C) The covered entity obtains the agreement to the disclosure from either:

(*1*) A parent, guardian, or other person acting *in loco parentis* of the individual, if the individual is an unemancipated minor; or

(*2*) The individual, if the individual is an adult or emancipated minor.

* * * * *

(e) * * *

(1) * * *

(iii) For the purposes of paragraph (e)(1)(ii)(A) of this section, a covered entity receives satisfactory assurances from a party seeking protected health information if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:

* * *

* * * * *

(vi) Notwithstanding paragraph (e)(1)(ii) of this section, a covered entity may disclose protected health information in response to lawful process described in paragraph (e)(1)(ii) of this section without receiving satisfactory assurance under paragraph (e)(1)(ii)(A) or (B) of this section, if the covered entity makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of paragraph (e)(1)(iii) of this section or to seek a qualified protective order sufficient to meet the requirements of paragraph (e)(1)(v) of this section.

* * * * *

(i) * * *

(2) * * *

(iii) *Protected health information needed.* A brief description of the protected health information for which use or access has been determined to be necessary by the IRB or privacy board, pursuant to paragraph (i)(2)(ii)(C) of this section;

* * * * *

(k) * * *

(1) * * *

(ii) *Separation or discharge from military service.* A covered entity that is a component of the Departments of Defense or Homeland Security may disclose to the Department of Veterans Affairs (DVA) the protected health information of an individual who is a member of the Armed Forces upon the separation or discharge of the individual from military service for the purpose of a determination by DVA of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs.

* * * * *

(3) *Protective services for the President and others.* A covered entity may disclose protected health information to authorized Federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056 or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879.

* * * * *

(5) * * *

(i) * * *

(E) Law enforcement on the premises of the correctional institution; or

* * * * *

47. In § 164.514, revise paragraphs (e)(4)(ii)(C)(*4*) and (f) to read as follows:

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

* * * * *

(e) * * *

(4) * * *

(ii) * * *

(C) * * *

(*4*) Ensure that any agents 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

* * * * *

(f) *Fundraising and remunerated treatment communications.*

(1)(i) *Standard: Uses and disclosures for fundraising.* Subject to the conditions of paragraph (f)(1)(ii) of this section, a covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization meeting the requirements of § 164.508:

(A) Demographic information relating to an individual; and

(B) Dates of health care provided to an individual.

(ii) *Implementation specifications: Fundraising requirements.* (A) A covered entity may not use or disclose protected health information for fundraising purposes as otherwise permitted by paragraph (f)(1)(i) of this section unless a statement required by § 164.520(b)(1)(iii)(B) is included in the covered entity's notice of privacy practices.

(B) With each fundraising communication sent to an individual under this paragraph, a covered entity must provide the individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications. The method for an individual to elect not to receive further fundraising communications may not cause the individual to incur an undue burden or more than a nominal cost.

(C) A covered entity may not condition treatment or payment on the individual's choice with respect to the receipt of fundraising communications.

(D) A covered entity may not send fundraising communications to an

individual under this paragraph where the individual has elected not to receive such communications under paragraph (f)(1)(ii)(B) of this section.

(2) *Standard: Uses and disclosures for remunerated treatment communications.* Where a covered health care provider receives financial remuneration, as defined in paragraph (3) of the definition of marketing at § 164.501, in exchange for making a treatment communication to an individual about a health-related product or service, such communication is not marketing and does not require an authorization meeting the requirements of § 164.508, only if the following requirements are met:

(i) The covered health care provider has included the information required by § 164.520(b)(1)(iii)(A) in its notice of privacy practices; and

(ii) The communication discloses the fact that the covered health care provider is receiving financial remuneration in exchange for making the communication and provides the individual with a clear and conspicuous opportunity to elect not to receive any further such communications. The method for an individual to elect not to receive further such communications may not cause the individual to incur an undue burden or more than a nominal cost.

* * * * *

48. In § 164.520, revise paragraphs (b)(1)(ii)(E), (b)(1)(iii), and (b)(1)(iv)(A) to read as follows:

§ 164.520 Notice of privacy practices for protected health information.

* * * * *

(b) * * *

(1) * * *

(ii) * * *

(E) A description of the types of uses and disclosures that require an authorization under § 164.508(a)(2)–(a)(4), a statement that other uses and disclosures not described in the notice will be made only with the individual's written authorization, and a statement that the individual may revoke an authorization as provided by § 164.508(b)(5).

(iii) *Separate statements for certain uses or disclosures.* If the covered entity intends to engage in any of the following activities, the description required by paragraph (b)(1)(ii)(A) of this section must include a separate statement informing the individual of such activities, as applicable:

(A) In accordance with § 164.514(f)(2), the covered health care provider may send treatment communications to the individual concerning treatment alternatives or other health-related products or services where the provider receives financial remuneration, as defined in paragraph (3) of the definition of marketing at § 164.501, in exchange for making the communications, and the individual has a right to opt out of receiving such communications;

(B) In accordance with § 164.514(f)(1), the covered entity may contact the individual to raise funds for the covered entity and the individual has a right to opt out of receiving such communications; or

(C) In accordance with § 164.504(f), the group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the sponsor of the plan.

(iv) * * *

(A) The right to request restrictions on certain uses and disclosures of protected health information as provided by § 164.522(a), including a statement that the covered entity is not required to agree to a requested restriction, except in case of a disclosure restricted under § 164.522(a)(1)(vi);

* * * * *

49. Amend § 164.522 as follows:

a. Revise paragraph (a)(1)(ii);

b. Add new paragraph (a)(1)(vi); and

c. Revise the introductory text of paragraph (a)(2), and paragraphs (a)(2)(iii), and paragraph (a)(3).

The revisions and additions read as follows:

§ 164.522 Rights to request privacy protection for protected health information.

(a)(1) * * *

(ii) Except as provided in paragraph (a)(1)(vi) of this section, a covered entity is not required to agree to a restriction.

* * * * *

(vi) A covered entity must agree to the request of an individual to restrict disclosure of protected health information about the individual to a health plan if:

(A) The disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and

(B) The protected health information pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full.

(2) *Implementation specifications: Terminating a restriction.* A covered entity may terminate a restriction, if:

* * * * *

(iii) The covered entity informs the individual that it is terminating its agreement to a restriction, except that such termination is:

(A) Not effective for protected health information restricted under paragraph (a)(1)(vi) of this section; and

(B) Only effective with respect to protected health information created or received after it has so informed the individual.

(3) *Implementation specification: Documentation.* A covered entity must document a restriction in accordance with § 160.530(j) of this subchapter.

* * * * *

50. Amend § 164.524 as follows:

a. Revise paragraph (c)(2)(i);

b. Redesignate paragraph (c)(2)(ii) as paragraph (c)(2)(iii);

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

d. Revise paragraphs (c)(3) and (c)(4)(i);

e. Redesignate paragraphs (c)(4)(ii) and (c)(4)(iii) as paragraphs (c)(4)(iii) and (c)(4)(iv), respectively; and

f. Add new paragraph (c)(4)(ii).

The revisions and additions read as follows:

§ 164.524 Access of individuals to protected health information.

* * * * *

(c) * * *

(2) *Form of access requested.* (i) The covered entity must provide the individual with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by the covered entity and the individual.

(ii) Notwithstanding paragraph (c)(2)(i) of this section, if the protected health information that is the subject of a request for access is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, the covered entity must provide the individual with access to the protected health information in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual.

* * * * *

(3) *Time and manner of access.* (i) The covered entity must provide the access as requested by the individual in a timely manner as required by paragraph (b)(2) of this section, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy of the protected health information at the individual's request. The covered entity may discuss the scope, format,

and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.

(ii) If an individual's request for access directs the covered entity to transmit the copy of protected health information directly to another person designated by the individual, the covered entity must provide the copy to the person designated by the individual. The individual's request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of protected health information.

(4) * * *

(i) Labor for copying the protected health information requested by the individual, whether in paper or electronic form;

(ii) Supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media;

* * * * *

51. In § 164.532, revise paragraphs (d), (e)(1) and (e)(2) to read as follows:

§ 164.532 Transition provisions.

* * * * *

(d) *Standard: Effect of prior contracts or other arrangements with business associates.* Notwithstanding any other provisions of this part, a covered entity, or business associate with respect to a subcontractor, 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 §§ 164.308(b), 164.314(a), 164.502(e), and 164.504(e), only in accordance with paragraph (e) of this section.

(e) *Implementation specification: Deemed compliance.* (1) *Qualification.* Notwithstanding other sections of this part, a covered entity, or business associate with respect to a subcontractor, is deemed to be in compliance with the documentation and contract requirements of §§ 164.308(b), 164.314(a), 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 [DATE OF PUBLICATION OF THE FINAL RULE IN THE FEDERAL REGISTER], such covered entity, or business associate with respect to a subcontractor, has entered into and is operating pursuant to a written contract or other written arrangement with the business associate that complies with the applicable provisions of §§ 164.314(a) or 164.504(e) that were in effect on such date; and

(ii) The contract or other arrangement is not renewed or modified from [DATE THAT IS 60 DAYS AFTER DATE OF PUBLICATION OF THE FINAL RULE IN THE FEDERAL REGISTER], until [DATE THAT IS 240 DAYS AFTER DATE OF PUBLICATION OF THE FINAL RULE IN THE FEDERAL REGISTER].

(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 [DATE THAT IS 240 DAYS AFTER DATE OF PUBLICATION OF THE FINAL RULE IN THE FEDERAL REGISTER]; or

(ii) [DATE THAT IS ONE YEAR AND 240 DAYS AFTER DATE OF PUBLICATION OF THE FINAL RULE IN THE FEDERAL REGISTER].

* * * * *

Dated: April 9, 2010.

Kathleen Sebelius,

Secretary.

Editorial Note: This document was received in the Office of the Federal Register on July 2, 2010.

[FR Doc. 2010–16718 Filed 7–8–10; 8:45 am]

BILLING CODE 4153–01–P