A covered entity may only extend the deadline one time per request for accounting.

The NPRM did not address whether a covered entity could charge a fee for the accounting of disclosures.

In the final rule, we provide that individuals have a right to receive one free accounting per 12 month period. For each additional request by an individual within the 12 month period, the covered entity may charge a reasonable, cost-based fee. If it imposes such a fee, the covered entity must inform the individual of the fee in advance and provide the individual with an opportunity to withdraw or modify the request in order to avoid or reduce the fee.

Procedures and Documentation

As in the proposed rule, we establish documentation requirements for covered entities subject to this provision. In accordance with § 164.530(j), for disclosures that are subject to the accounting requirement, the covered entity must retain documentation of the information required to be included in the accounting. The covered entity must also retain a copy of any accounting provided and must document the titles of the persons or offices responsible for receiving and processing requests for an accounting.

Section 164.530—Administrative Requirements

Designation of a Privacy Official and Contact Person

In § 164.518(a) of the NPRM, we proposed that covered entities be required to designate an individual as the covered entity's privacy official, responsible for the implementation and development of the entity's privacy policies and procedures. We also proposed that covered entities be required to designate a contact person to receive complaints about privacy and provide information about the matters covered by the entity's notice. We indicated that the contact person could be, but was not required to be, the person designated as the privacy official. We proposed to leave implementation details to the discretion of the covered entity. We expected implementation to vary widely depending on the size and nature of the covered entity, with small offices assigning this as an additional duty to an existing staff person, and large organizations creating a full-time privacy official. In proposed § 164.512, we also proposed to require the covered plan or provider's privacy notice to include the name of a contact person for privacy matters.

The final regulation retains the requirements for a privacy official and contact person as specified in the NPRM. These designations must be documented. The designation of privacy official and contact person positions within affiliated entities will depend on how the covered entity chooses to designate the covered entity(ies) under § 164.504(b). If a subsidiary is defined as a covered entity under this regulation, then a separate privacy official and contact person is required for that covered entity. If several subsidiaries are designated as a single covered entity, pursuant to § 164.504(b), then together they need have only a single privacy officer and contact person. If several covered entities share a notice for services provided on the same premises, pursuant to § 164.520(d), that notice need designate only one privacy official and contact person for the information collected under that notice.

These requirements are consistent with the approach recommended by the Joint Commission on Accreditation of Healthcare Organizations, and the National Committee for Quality Assurance, in its paper ''Protecting Personal Health Information; A framework for Meeting the Challenges in a Managed Care Environment.'' This paper notes that ''accountability is enhanced by having focal points who are responsible for assessing compliance with policies and procedures * * * '' (p. 29)

Training

In § 164.518(b) of the NPRM we proposed to require that covered entities provide training on the entities' policies and procedures to all members of the workforce likely to have access to protected health information. Each entity would be required to provide initial training by the date on which this rule became applicable. After that date, each covered entity would have to provide training to new members of the workforce within a reasonable time after joining the entity. In addition, we proposed that when a covered entity made material changes in its privacy policies or procedures, it would be required to retrain those members of the workforce whose duties were related to the change within a reasonable time of making the change.

The NPRM would have required that, upon completion of the training, the trainee would be required to sign a statement certifying that he or she received the privacy training and would honor all of the entity's privacy policies and procedures. Entities would determine the most effective means of achieving this training requirement for their workforce. We also proposed that, at least every three years after the initial training, covered entities would be required to have each member of the workforce sign a new statement certifying that he or she would honor all of the entity's privacy policies and procedures. The covered entity would have been required to document its policies and procedures for complying with the training requirements.

The final regulation requires covered entities to train all members of their workforce on the policies and procedures with respect to protected health information required by this rule, as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity. We do not change the proposed time lines for training existing and new members of the workforce, or for training due to material changes in the covered entity's policies and procedures. We eliminate both the requirement for employees to sign a certification following training and the triennial re-certification requirement. Covered entities are responsible for implementing policies and procedures to meet these requirements and for documenting that training has been provided.

Safeguards

In § 164.518(c) of the NPRM, we proposed to require covered entities to put in place administrative, technical, and physical safeguards to protect the privacy of protected health information. We made reference in the preamble to similar requirements proposed for certain electronic information in the Notice of Proposed Rulemaking entitled the Security and Electronic Signature Standards (HCFA–0049–P). We stated that we were proposing parallel and consistent requirements for safeguarding the privacy of protected health information. In § 164.518(c)(3) of the NPRM, we required covered entities to have safeguards to ensure that information was not used in violation of the requirements of this subpart or by people who did not have proper authorization to access the information.

We do not change the basic proposed requirements that covered entities have administrative, technical and physical safeguards to protect the privacy of protected health information. We combine the proposed requirements into a single standard that requires covered entities to safeguard protected health information from accidental or intentional use or disclosure that is a violation of the requirements of this rule

and to protect against the inadvertent disclosure of protected health information to persons other than the intended recipient. Limitations on access to protected health information by the covered entities workforce will also be covered by the policies and procedures for ''minimum necessary'' use of protected health information, pursuant to § 164.514(d). We expect these provisions to work in tandem.

We do not prescribe the particular measures that covered entities must take to meet this standard, because the nature of the required policies and procedures will vary with the size of the covered entity and the type of activities that the covered entity undertakes. (That is, as with other provisions of this rule, this requirement is ''scalable.'') Examples of appropriate safeguards include requiring that documents containing protected health information be shredded prior to disposal, and requiring that doors to medical records departments (or to file cabinets housing such records) remain locked and limiting which personnel are authorized to have the key or pass-code. We intend this to be a common sense, scalable, standard. We do not require covered entities to guarantee the safety of protected health information against all assaults. Theft of protected health information may or may not signal a violation of this rule, depending on the circumstances and whether the covered entity had reasonable policies to protect against theft. Organizations such as the Association for Testing and Materials (ASTM) and the American Health Information Management Association (AHIMA) have developed a body of recommended practices for handling of protected health information that covered entities may find useful.

We note that the proposed HIPAA Security Standards would require covered entities to safeguard the privacy and integrity of health information. For electronic information, compliance with both regulations will be required.

In § 164.518(c)(2) of the NPRM we proposed requirements for verification procedures to establish identity and authority for permitted disclosures of protected health information.

In the final rule, this material has been moved to § 164.514(h).

Use or Disclosure of Protected Health Information by Whistleblowers

In § 164.518(c)(4) of the NPRM, this provision was entitled ''Implementation Specification: Disclosures by whistleblowers.'' It is now retitled ''Disclosures by whistleblowers,'' with certain changes, and moved to § 164.502(j)(1).

Complaints to the Covered Entity

In § 164.518(d) of the NPRM, we proposed to require covered entities to have a mechanism for receiving complaints from individuals regarding the health plan's or provider's compliance with the requirements of this proposed rule. We did not require that the health plan or provider develop a formal appeals mechanism, nor that ''due process'' or any similar standard be applied. Additionally, there was no requirement to respond in any particular manner or time frame.

We proposed two basic requirements for the complaint process. First, the covered health plan or health care provider would be required to identify in the notice of information practices a contact person or office for receiving complaints. Second, the health plan or provider would be required to maintain a record of the complaints that are filed and a brief explanation of their resolution, if any.

In the final rule, we retain the requirement for an internal complaint process for compliance with this rule, including the two basic requirements of identifying a contact person and documenting complaints received and their dispositions, if any. We expand the scope of complaints that covered entities must have a means of receiving to include complaints concerning violations of the covered entity's privacy practices, not just violations of the rule. For example, a covered entity must have a mechanism for receiving a complaint that patient information is used at a nursing station in a way that it can also be viewed by visitors to the hospital, regardless of whether the practices at the nursing stations might constitute a violation of this rule.

Sanctions

In § 164.518(e) of the NPRM, we proposed to require all covered entities to develop, and apply when appropriate, sanctions against members of its workforce who failed to comply with privacy policies or procedures of the covered entity or with the requirements of the rule. Covered entities would be required to develop and impose sanctions appropriate to the nature of the violation. The preamble stated that the type of sanction applied would vary depending on factors such as the severity of the violation, whether the violation was intentional or unintentional, and whether the violation indicated a pattern or practice of improper use or disclosure of protected health information. Sanctions could range from a warning to termination. The NPRM preamble language also stated that covered entities would be required to apply sanctions against business associates that violated the proposed rule.

In the final rule, we retain the requirement for sanctions against members of a covered entity's workforce. We also require a covered entity to have written policies and procedures for the application of appropriate sanctions for violations of this subpart and to document those sanctions. These sanctions do not apply to whistleblower activities that meet the provisions of § 164.502(j) or complaints, investigations, or opposition that meet the provisions of § 164.530(g)(2). We eliminate language regarding business associates from this section. Requirements with respect to business associates are stated in § 164.504.

Duty To Mitigate

In proposed § 164.518(f), we would have required covered entities to have policies and procedures for mitigating, to the extent practicable, any deleterious effect of a use or disclosure of protected health information in violation of the requirements of this subpart. The NPRM preamble also included specific language applying this requirement to harm caused by members of the covered entity's workforce and business associates.

With respect to business associates, the NPRM preamble but not the NPRM rule text, stated that covered entities would have a duty to take reasonable steps in response to breaches of contract terms. Covered entities generally would not be required to monitor the activities of their business associates, but would be required to take steps to address problems of which they become aware, and, where the breach was serious or repeated, would also be required to monitor the business associate's performance to ensure that the wrongful behavior had been remedied. Termination of the arrangement would be required only if it became clear that a business associate could not be relied upon to maintain the privacy of protected health information provided to it.

In the final rule, we clarify this requirement by imposing a duty for covered entities to mitigate any harmful effect of a use or disclosure of protected health information that is known to the covered entity. We apply the duty to mitigate to a violation of the covered entity's policies and procedures, not just a violation of the requirements of the subpart. We resolve the ambiguities in the NPRM by imposing this duty on covered entities for harm caused by

either members of their workforce or by their business associates.

We eliminate the language regarding potential breaches of business associate contracts from this section. All other requirements with respect to business associates are stated in § 164.504.

Refraining from Intimidating or Retaliatory Acts

In § 164.522(d)(4) of the NPRM, in the Compliance and Enforcement section, we proposed that one of the responsibilities of a covered entity would be to refrain from intimidating or retaliatory acts. Specifically, the rule provided that ''[a] covered entity may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the filing of a complaint under this section, for testifying, assisting, participating in any manner in an investigation, compliance review, proceeding or hearing under this Act, or opposing any act or practice made unlawful by this subpart.''

In the final rule, we continue to require that entities refrain from intimidating or retaliatory acts; however, the provisions have been moved to the Administrative Requirements provisions in § 164.530. This change is not just clerical; in making this change, we apply this provision to the privacy rule alone rather than to all the HIPAA administrative simplification rules. (The compliance and enforcement provisions that were in § 164 are now in Part 160, Subpart C.)

We continue to prohibit retaliation against individuals for filing a complaint with the Secretary, but also prohibit retaliation against any other person who files such a complaint. This is the case because the term ''individual'' is generally limited to the person who is the subject of the information. The final rule prohibits retaliation against persons, not just individuals, for testifying, assisting, or participating in an investigation, compliance review, proceeding or hearing under Part C of Title XI. The proposed regulation referenced the ''Act,'' which is defined in Part 160 as the Social Security Act. Because we only intend to protect activities such as participation in investigations and hearings under the Administrative Simplification provisions of HIPAA, the final rule references Part C of Title XI of the Social Security Act.

The proposed rule would have prohibited retaliatory actions against individuals for opposing any act or practice made unlawful by this subpart. The final rule retains this provision, but applies it to any person, only if the person ''has a good faith belief that the practice opposed is unlawful, the manner of the opposition is reasonable and does not involve a disclosure of protected health information in violation of this subpart.'' The final rule provides additional protections, which had been included in the preamble to the proposed rule. Specifically, we prohibit retaliatory actions against individuals who exercise any right, or participate in any process established by the privacy rule (Part 164 Subpart E), and include as an example the filing of a complaint with the covered entity.

Waiver of Rights

In the final regulation, but not in the proposed regulation, we provide that a covered entity may not require individuals to waive their rights to file a complaint with the Secretary or their other rights under this rule as a condition of the provision of treatment, payment, enrollment in a health plan or eligibility for benefits. This provision ensures that covered entities do not take away the rights that individuals have been provided in Parts 160 and 164.

Requirements for Policies and Procedures, and Documentation Requirements

In § 164.520 of the NPRM, we proposed to require covered entities to develop and document their policies and procedures for implementing the requirements of the rule. In the final regulation we retain this approach, but specify which standards must be documented in each of the relevant sections. In this section, we state the general administrative requirements applicable to all policies and procedures required throughout the regulation.

In § 164.530(i), (j), and (k) of the final rule, we amend the NPRM language in several respects. In § 164.530(i) we require that the policies and procedures be reasonably designed to comply with the standards, implementation specifications, and other requirements of the relevant part of the regulation, taking into account the size of the covered entity and the nature of the activities undertaken by the covered entity that relate to protected health information. However, we clarify that the requirements that policies and procedures be reasonably designed may not be interpreted to permit or excuse any action that violates the privacy regulation. Where the covered entity has stated in its notice that it reserves the right to change information practices, we allow the new practice to apply to information created or collected prior to the effective date of the new practice and establish requirements for making this change. We also establish the conditions for making changes if the covered entity has not reserved the right to change its practices.

We require covered entities to modify in a prompt manner their policies and procedures to comply with changes in relevant law and, where the change also affects the practices stated in the notice, to change the notice. We make clear that nothing in our requirements regarding changes to policies and procedures or changes to the notice may be used by a covered entity to excuse a failure to comply with applicable law.

In § 164.530(j), we require that the policies and procedures required throughout the regulation be maintained in writing, and that any other communication, action, activity, or designation that must be documented under this regulation be documented in writing. We note that ''writing'' includes electronic storage; paper records are not required. We also note that, if a covered entity is required to document the title of a person, we mean the job title or similar description of the relevant position or office.

We require covered entities to retain any documentation required under this rule for at least six years (the statute of limitations period for the civil penalties) from the date of the creation of the documentation, or the date when the document was last in effect, which ever is later. This generalizes the NPRM provision to cover all documentation required under the rule. The language on ''last was in effect'' is a change from the NPRM which was worded ''unless a longer period applies under this subpart.''

This approach is consistent with the approach recommended by the Joint Commission on Accreditation of Healthcare Organizations, and the National Committee for Quality Assurance, in its paper ''Protecting Personal Health Information; A framework for Meeting the Challenges in a Managed Care Environment.'' This paper notes that ''MCOs [Managed Care Organizations] should have clearly defined policies and procedures for dealing with confidentiality issues.'' (p. 29).

Standards for Certain Group Health Plans

We add a new provision (§ 164.530(k)) to clarify the administrative responsibilities of group health plans that offer benefits through issuers and HMOs. Specifically, a group health plan that provides benefits solely through an issuer or HMO, and that does not create, receive or maintain protected health

information other than summary health information or information regarding enrollment and disenrollment, is not subject to the requirements of this section regarding designation of a privacy official and contact person, workforce training, safeguards, complaints, mitigation, or policies and procedures. Such a group health plan is only subject to the requirements of this section regarding documentation with respect to its plan documents. Issuers and HMOs are covered entities under this rule, and thus have independent obligations to comply with this section with respect to the protected health information they maintain about the enrollees in such group health plans. The group health plans subject to this provision will have only limited protected health information. Therefore, imposing these requirements on the group health plan would impose burdens not outweighed by a corresponding enhancement in privacy protections.

Section 164.532—Transition Provisions

In the NPRM, we did not address the effect of the regulation on consents and authorizations covered entities obtained prior to the compliance date of the regulation.

In the final rule, we clarify that, in certain circumstances, a covered entity may continue to rely upon consents, authorizations, or other express legal permissions obtained prior to the compliance date of this regulation to use or disclose protected health information even if these consents, authorizations, or permissions do not meet the requirements set forth in §§ 164.506 or 164.508.

We realize that a covered entity may wish to rely upon a consent, authorization, or other express legal permission obtained from an individual prior to the compliance date of this regulation which permits the use or disclosure of individually identifiable health information for activities that come within treatment, payment, or health care operations (as defined in § 164.501), but that do not meet the requirements for consents set forth in § 164.506. In the final rule, we permit a covered entity to rely upon such consent, authorization, or permission to use or disclose protected health information that it created or received before the applicable compliance date of the regulation to carry out the treatment, payment, or health care operations as long as it meets two requirements. First, the covered entity may not make any use or disclosure that is expressly excluded from the consent, authorization, or permission. Second, the covered entity must comply with all limitations expressed in the consent, authorization, or permission. Thus, we do not require a covered entity to obtain a consent that meets the requirements of § 164.506 to use or disclose this previously obtained protected health information as long as the use or disclosure is consistent with the requirements of this section. However, a covered entity will need to obtain a consent that meets the requirements of § 164.506 to the extent that it is required to obtain a consent under § 164.506 from an individual before it may use or disclose any protected health information it creates or receives after the date by which it must comply with this rule.

Similarly, we recognize that a covered entity may wish to rely upon a consent, authorization, or other express legal permission obtained from an individual prior to the applicable compliance date of this regulation that specifically permits the covered entity to use or disclose individually identifiable health information for activities other than to carry out treatment, payment, or health care operations. In the final rule, we permit a covered entity to rely upon such a consent, authorization, or permission to use or disclose protected health information that it created or received before the applicable compliance date of the regulation for the specific activities described in the consent, authorization, or permission as long as the covered entity complies with two requirements. First, the covered entity may not make any use or disclosure that is expressly excluded from the consent, authorization, or permission. Second, the covered entity must comply with all limitations expressed in the consent, authorization, or permission. Thus, we do not required a covered entity to obtain an authorization that meets the requirements of § 164.508 to use or disclose this previously obtained protected health information so long as the use or disclosure is consistent with the requirements of this section. However, a covered entity will need to obtain an authorization that meets the requirements of § 164.508, to the extent that it is required to obtain an authorization under this rule, from an individual before it may use or disclose any protected health information it creates or receives after the date by which it must comply with this rule.

Additionally, the final rule acknowledges that covered entities may wish to rely upon consents, authorizations, or other express legal permission obtained from an individual prior to the applicable compliance date for a specific research project that includes the treatment of individuals, such as clinical trials. These consents, authorizations, or permissions may specifically permit a use or disclosure of individually identifiable health information for purposes of the project. Alternatively, they may be general consents to participate in the project. A covered entity may use or disclose protected health information it created or received before or after to the applicable compliance date of this rule for purposes of the project provided that the covered entity complies with all limitations expressed in the consent, authorization, or permission.

If, pursuant to this section, a covered entity relies upon a previously obtained consent, authorization, or other express legal permission and agrees to a request for a restriction by an individual under § 164.522(a), any subsequent use or disclosure under that consent, authorization, or permission must comply with the agreed upon restriction as well.

We believe it is necessary to grandfather in previously obtained consents, authorizations, or other express legal permissions in these circumstances to ensure that important functions of the health care system are not impeded. We link the effectiveness of such consents, authorizations, or permissions in these circumstances to the applicable compliance date to give covered entities sufficient notice of the requirements set forth in §§ 164.506 and 164.508.

The rule does not change the past effectiveness of consents, authorizations, or other express legal permissions that do not come within this section. This means that uses or disclosures of individually identifiable health information made prior to the compliance date of this regulation are not subject to sanctions, even if they were made pursuant to documents or permissions that do not meet the requirements of this rule or were made without permission. This rule alters only the future effectiveness of the previously obtained consents, authorizations, or permissions. Covered entities are not required to rely upon these consents, authorizations, or permissions and may obtain new consents or authorizations that meet the applicable requirements of §§ 164.506 and 164.508.

When reaching this decision, we considered requiring all covered entities to obtain new consents or authorizations consistent with the requirements of §§ 164.506 and 164.508 before they would be able to use or disclose protected health information obtained

after the compliance date of these rules. We rejected this option because we recognize that covered entities may not always be able to obtain new consents or authorizations consistent with the requirements of §§ 164.506 and 164.508 from all individuals upon whose information they rely. We also refrained from impeding the rights of covered entities to exercise their interests in the records they have created. We do not require covered entities with existing records or databases to destroy or remove the protected health information for which they do not have valid consents or authorizations that meet the requirements of §§ 164.506 and 164.508. Covered entities may rely upon the consents, authorizations, or permissions they obtained from individuals prior to the applicable compliance date of this regulation consistent with the constraints of those documents and the requirements discussed above.

We note that if a covered entity obtains before the applicable compliance date of this regulation a consent that meets the requirements of § 164.506, an authorization that meets the requirements of § 164.508, or an IRB or privacy board waiver of authorization that meets the requirements of § 164.512(i), the consent, authorization, or waiver is effective for uses or disclosures that occur after the compliance date and that are consistent with the terms of the consent, authorization, or waiver.

Section 164.534—Compliance Dates for Initial Implementation of the Privacy Standards

In the NPRM, we provided that a covered entity must be in compliance with this subpart not later than 24 months following the effective date of this rule, except that a covered entity that is a small health plan must be in compliance with this subpart not later than 36 months following the effective date of the rule.

The final rule did not make any substantive changes. The format is changed so as to more clearly present the various compliance dates. The final rule lists the types of covered entities and then the various dates that would apply to each of these entities.

III. Section-by-Section Discussion of Comments

The following describes the provisions in the final regulation, and the changes we make to the proposed provisions section-by-section. Following each section are our responses to the comments to that section. This section of the preamble is organized to follow the corresponding section of the final rule, not the NPRM.

General Comments

We received many comments on the rule overall, not to a particular provision. We respond to those comments here. Similar comments, but directed to a specific provision in the proposed rule, are answered below in the corresponding section of this preamble.

Comments on the Need for Privacy Standards, and Effects of this Regulation on Current Protections

Comment: Many commenters expressed the opinion that federal legislation is necessary to protect the privacy of individuals' health information. One comment advocated Congressional efforts to provide a comprehensive federal health privacy law that would integrate the substance abuse regulations with the privacy regulation.

Response: We agree that comprehensive privacy legislation is urgently needed. This administration has urged the Congress to pass such legislation. While this regulation will improve the privacy of individuals' health information, only legislation can provide the full array of privacy protection that individuals need and deserve.

Comment: Many commenters noted that they do not go to a physician, or do not completely share health information with their physician, because they are concerned about who will have access to that information. Many physicians commented on their patients' reluctance to share information because of fear that their information will later be used against them.

Response: We agree that strong federal privacy protections are necessary to enhance patients' trust in the health care system.

Comment: Many commenters expressed concerns that this regulation will allow access to health information by those who today do not have such access, or would allow their physician to disclose information which may not lawfully be disclosed today. Many of these commenters stated that today, they consent to every disclosure of health information about them, and that absent their consent the privacy of their health information is ''absolute.'' Others stated that, today, health information is disclosed only pursuant to a judicial order. Several commenters were concerned that this regulation would override stronger state privacy protection.

Response: This regulation does not, and cannot, reduce current privacy protections. The statutory language of the HIPAA specifically mandates that this regulation does not preempt state laws that are more protective of privacy.

As discussed in more detail in later this preamble, while many people believe that they must be asked permission prior to any release of health information about them, current laws generally do not impose such a requirement. Similarly, as discussed in more detail later in this preamble, judicial review is required today only for a small proportion of releases of health information.

Comment: Many commenters asserted that today, medical records ''belong'' to patients. Others asserted that patients own their medical information and health care providers and insurance companies who maintain health records should be viewed as custodians of the patients' property.

Response: We do not intend to change current law regarding ownership of or responsibility for medical records. In developing this rule we reviewed current law on this and related issues, and built on that foundation.

Under state laws, medical records are often the property of the health care provider or medical facility that created them. Some state laws also provide patients with access to medical records or an ownership interest in the health information in medical records. However, these laws do not divest the health care provider or the medical facility of its ownership interest in medical records. These statutes typically provide a patient the right to inspect or copy health information from the medical record, but not the right to take the provider's original copy of an item in the medical record. If a particular state law provides greater ownership rights, this regulation leaves such rights in place.

Comment: Some commenters argued that the use and disclosure of sensitive personal information must be strictly regulated, and violation of such regulations should subject an entity to significant penalties and sanctions.

Response: We agree, and share the commenters' concern that the penalties in the HIPAA statute are not sufficient to fully protect individuals' privacy interests. The need for stronger penalties is among the reasons we believe Congress should pass comprehensive privacy legislation.

Comment: Many commenters expressed the opinion that the proposed ruled should provide stricter privacy protections.

Response: We received nearly 52,000 comments on the proposed regulation, and make substantial changes to the proposal in response to those comments. Many of these changes will strengthen the protections that were proposed in the NPRM.

Comment: Many comments express concerns that their health information will be given to their employers.

Response: We agree that employer access to health information is a particular concern. In this final regulation, we make significant changes to the NPRM that clarify and provide additional safeguards governing when and how the health plans covered by this regulation may disclose health information to employers.

Comment: Several commenters argued that individuals should be able to sue for breach of privacy.

Response: We agree, but do not have the legislative authority to grant a private right of action to sue under this statute. Only Congress can grant that right.

Objections to Government Access to Protected Health Information

Comment: Many commenters urged the Department not to create a government database of health information, or a tracking system that would enable the government to track individuals health information.

Response: This regulation does not create such a database or tracking system, nor does it enable future creation of such a database. This regulation describes the ways in which health plans, health care clearinghouses, and certain health care providers may use and disclose identifiable health information with and without the individual's consent.

Comment: Many commenters objected to government access to or control over their health information, which they believe the proposed regulation would provide.

Response: This regulation does not increase current government access to health information. This rule sets minimum privacy standards. It does not require disclosure of health information, other than to the subject of the records or for enforcement of this rule. Health plans and health care providers are free to use their own professional ethics and judgement to adopt stricter policies for disclosing health information.

Comment: Some commenters viewed the NPRM as creating fewer hurdles for government access to protected health information than for access to protected health information by private organizations. Some health care providers commented that the NPRM would impose substantial new restrictions on private sector use and disclosure of protected health information, but would make government access to protected health information easy. One consumer advocacy group made the same observation.

Response: We acknowledge that many of the national priority purposes for which we allow disclosure of protected health information without consent or authorization are for government functions, and that many of the governmental recipients of such information are not governed by this rule. It is the role of government to undertake functions in the broader public interest, such as public health activities, law enforcement, identification of deceased individuals through coroners' offices, and military activities. It is these public purposes which can sometimes outweigh an individual's privacy interest. In this rule, we specify the circumstances in which that balance is tipped toward the public interest with respect to health information. We discuss the rationale behind each of these permitted disclosures in the relevant preamble sections below.

Miscellaneous Comments

Comment: Many commenters objected to the establishment of a unique identifier for health care or other purposes.

Response: This regulation does not create an identifier. We assume these comments refer to the unique health identifier that Congress directed the Secretary to promulgate under section1173(b) of the Social Security Act, added by section 262 of the HIPAA. Because of the public concerns about such an identifier, in the summer of 1998 Vice President Gore announced that the Administration would not promulgate such a regulation until comprehensive medical privacy protections were in place. In the fall of that year, Congress prohibited the Department from promulgating such an identifier, and that prohibition remains in place. The Department has no plans to promulgate a unique health identifier.

Comment: Many commenters asked that we withdraw the proposed regulation and not publish a final rule.

Response: Under section 264 of the HIPAA, the Secretary is required by Congress to promulgate a regulation establishing standards for health information privacy. Further, for the reasons explained throughout this preamble above, we believe that the need to protect health information privacy is urgent and that this regulation is in the public's interest.

Comment: Many commenters express the opinion that their consent should be required for all disclosure of their health information.

Response: We agree that consent should be required prior to release of health information for many purposes, and impose such a requirement in this regulation. Requiring consent prior to all release of health information, however, would unduly jeopardize public safety and make many operations of the health care system impossible. For example, requiring consent prior to release of health information to a public health official who is attempting to track the source of an outbreak or epidemic could endanger thousands of lives. Similarly, requiring consent before an oversight official could audit a health plan would make detection of health care fraud all but impossible; it could take health plans months or years to locate and obtain the consent of all current and past enrollees, and the health plan would not have a strong incentive to do so. These uses of medical information are clearly in the public interest.

In this regulation, we must balance individuals' privacy interests against the legitimate public interests in certain uses of health information. Where there is an important public interest, this regulation imposes procedural safeguards that must be met prior to release of health information, in lieu of a requirement for consent. In some instances the procedural safeguards consist of limits on the circumstances in which information may be disclosed, in others the safeguards consist of limits on what information may be disclosed, and in other cases we require some form of legal process (*e.g.,* a warrant or subpoena) prior to release of health information. We also allow disclosure of health information without consent where other law mandates the disclosures. Where such other law exists, another public entity has made the determination that the public interests outweigh the individual's privacy interests, and we do not upset that determination in this regulation. In short, we tailor the safeguards to match the specific nature of the public purpose. The specific safeguards are explained in each section of this regulation below.

Comment: Many comments address matters not relevant to this regulation, such as alternative fuels, hospital reimbursement, and gulf war syndrome.

Response: These and similar matters are not relevant to this regulation and will not be addressed further.

Comment: A few commenters questioned why this level of detail is needed in response to the HIPAA Congressional mandate.

Response: This level of detail is necessary to ensure that individuals' rights with respect to their health information are clear, while also ensuring that information necessary for important public functions, such as protecting public health, promoting biomedical research, fighting health care fraud, and notifying family members in disaster situations, will not be impaired by this regulation. We designed this rule to reflect current practices and change some of them. The comments and our fact finding revealed the complexity of current health information practices, and we believe that the complexity entailed in reflecting those practices is better public policy than a perhaps simpler rule that disturbed important information flows.

Comment: A few comments stated that the goal of administrative simplification should never override the privacy of individuals.

Response: We believe that privacy is a necessary component of administrative simplification, not a competing interest.

Comment: At least one commenter said that the goal of administrative simplification is not well served by the proposed rule.

Response: Congress recognized that privacy is a necessary component of administrative simplification. The standardization of electronic health information mandated by the HIPAA that make it easier to share that information for legitimate purposes also make the inappropriate sharing of that information easier. For this reason, Congress included a mandate for privacy standards in this section of the HIPAA. Without appropriate privacy protections, public fear and instances of abuse would make it impossible for us to take full advantage of the administrative and costs benefits inherent in the administrative simplification standards.

Comment: At least one commenter asked us to require psychotherapists to assert any applicable legal privilege on patients' behalf when protected health information is requested.

Response: Whether and when to assert a claim of privilege on a patient's behalf is a matter for other law and for the ethics of the individual health care provider. This is not a decision that can or should be made by the federal government.

Comment: One commenter called for HHS to consider the privacy regulation in conjunction with the other HIPAA standards. In particular, this comment focused on the belief that the Security Standards should be compatible with the existing and emerging health care and information technology industry standards.

Response: We agree that both this regulation and the final Security Regulation should be compatible with existing and emerging technology industry standards. This regulation is ''technology neutral.'' We do not mandate the use of any particular technologies, but rather set standards which can be met through a variety of means.

Comment: Several commenters claimed that the statutory authority given under HIPAA cannot provide meaningful privacy protections because many entities with access to protected health information, such as employers, worker's compensation carriers, and life insurance companies, are not covered entities. These commenters expressed support for comprehensive legislation to close many of the existing loopholes.

Response: We agree with the commenters that comprehensive legislation is necessary to provide full privacy protection and have called for members of Congress to pass such legislation to prevent unauthorized and potentially harmful uses and disclosures of information.

Part 160—Subpart A—General Provisions

Section 160.103—Definitions

Business Associate

The response to comments on the definition of ''business partner,'' renamed in this rule as ''business associate,'' is included in the response to comments on the requirements for business associates in the preamble discussion of § 164.504.

Covered Entity

Comment: A number of commenters urged the Department to expand or clarify the definition of ''covered entity'' to include certain entities other than health care clearinghouses, health plans, and health care providers who conduct standard transactions. For example, several commenters asked that the Department generally expand the scope of the rule to cover all entities that receive or maintain individually identifiable health information; others specifically urged the Department to cover employers, marketing firms, and legal entities that have access to individually identifiable health information. Some commenters asked that life insurance and casualty insurance carriers be considered covered entities for purposes of this rule. One commenter recommended that Pharmacy Benefit Management (PBM) companies be considered covered entities so that they may use and disclose protected health information without authorization.

In addition, a few commenters asked the Department to clarify that the definition includes providers who do not directly conduct electronic transactions if another entity, such as a billing service or hospital, does so on their behalf.

Response: We understand that many entities may use and disclose individually identifiable health information. However, our jurisdiction under the statute is limited to health plans, health care clearinghouses, and health care providers who transmit any health information electronically in connection with any of the standard financial or administrative transactions in section 1173(a) of the Act. These are the entities referred to in section 1173(a)(1) of the Act and thus listed in § 160.103 of the final rule. Consequently, once protected health information leaves the purview of one of these covered entities, their business associates, or other related entities (such as plan sponsors), the information is no longer afforded protection under this rule. We again highlight the need for comprehensive federal legislation to eliminate such gaps in privacy protection.

We also provide the following clarifications with regard to specific entities.

We clarify that employers and marketing firms are not covered entities. However, employers may be plan sponsors of a group health plan that is a covered entity under the rule. In such a case, specific requirements apply to the group health plan. See the preamble on § 164.504 for a discussion of specific ''firewall'' and other organizational requirements for group health plans and their employer sponsors. The final rule also contains provisions addressing when an insurance issuer providing benefits under a group health plan may disclose summary health information to a plan sponsor.

With regard to life and casualty insurers, we understand that such benefit providers may use and disclose individually identifiable health information. However, Congress did not include life insurers and casualty insurance carriers as ''health plans'' for the purposes of this rule and therefore they are not covered entities. See the discussion regarding the definition of ''health plan'' and excepted benefits.

In addition, we clarify that a PBM is a covered entity only to the extent that it meets the definition of one or more of the entities listed in § 160.102. When providing services to patients through managed care networks, it is likely that a PBM is acting as a business associate of a health plan, and may thus use and disclose protected health information pursuant to the relevant provisions of this rule. PBMs may also be business associates of health care providers. See the preamble sections on §§ 164.502, 164.504, and 164.506 for discussions of the specific requirements related to business associates and consent.

Lastly, we clarify that health care providers who do not submit HIPAA transactions in standard form become covered by this rule when other entities, such as a billing service or a hospital, transmit standard electronic transactions on their behalf. The provider could not circumvent these requirements by assigning the task to a contractor.

Comment: Many commenters urged the Department to restrict or clarify the definition of ''covered entity'' to exclude certain entities, such as department-operated hospitals (public hospitals); state Crime Victim Compensation Programs; employers; and certain lines of insurers, such as workers' compensation insurers, property and casualty insurers, reinsurers, and stop-loss insurers. One commenter expressed concern that clergy, religious practitioners, and other faith-based service providers would have to abide by the rule and asked that the Department exempt prayer healing and non-medical health care.

Response: The Secretary provides the following clarifications in response to these comments. To the extent that a ''department-operated hospital'' meets the definition of a ''health care provider'' and conducts any of the standard transactions, it is a covered entity for the purposes of this rule. We agree that a state Crime Victim Compensation Program is not a covered entity if it is not a health care provider that conducts standard transactions, health plan, or health care clearinghouse. Further, as described above, employers are not covered entities.

In addition, we agree that workers' compensation insurers, property and casualty insurers, reinsurers, and stop-loss insurers are not covered entities, as they do not meet the statutory definition of ''health plan.'' See further discussion in the preamble on § 160.103 regarding the definition of ''health plan.'' However, activities related to ceding, securing, or placing a contract for reinsurance, including stop-loss insurance, are health care operations in the final rule. As such, reinsurers and stop-loss insurers may obtain protected health information from covered entities.

Also, in response to the comment regarding religious practitioners, the Department clarifies that ''health care'' as defined under the rule does not include methods of healing that are solely spiritual. Therefore, clergy or other religious practitioners that provide solely religious healing services are not health care providers within the meaning of this rule, and consequently not covered entities for the purposes of this rule.

Comment: A few commenters expressed general uncertainty and requested clarification as to whether certain entities were covered entities for the purposes of this rule. One commenter was uncertain as to whether the rule applies to certain social service entities, in addition to clinical social workers that the commenter believes are providers. Other commenters asked whether researchers or non-governmental entities that collect and analyze patient data to monitor and evaluate quality of care are covered entities. Another commenter requested clarification regarding the definition's application to public health agencies that also are health care providers as well as how the rule affects public health agencies in their data collection from covered entities.

Response: Whether the professionals described in these comments are covered by this rule depends on the activities they undertake, not on their profession or degree. The definitions in this rule are based on activities and functions, not titles. For example, a social service worker whose activities meet this rule's definition of health care will be a health care provider. If that social service worker also transmits information in a standard HIPAA transaction, he or she will be a covered health entity under this rule. Another social service worker may provide services that do not meet the rule's definition of health care, or may not transmit information in a standard transaction. Such a social service worker is not a covered entity under this rule. Similarly, researchers in and of themselves are not covered entities. However, researchers may also be health care providers if they provide health care. In such cases, the persons, or entities in their role as health care providers may be covered entities if they conduct standard transactions.

With regard to public health agencies that are also health care providers, the health care provider ''component'' of the agency is the covered entity if that component conducts standard transactions. See discussion of ''health care components'' below. As to the data collection activities of a public health agency, the final rule in § 164.512(b) permits a covered entity to disclose protected health information to public health authorities under specified circumstances, and permits public health agencies that are also covered entities to use protected health information for these purposes. See § 164.512(b) for further details.

Comment: A few commenters requested that the Department clarify that device manufacturers are not covered entities. They stated that the proposal did not provide enough guidance in cases where the ''manufacturer supplier'' has only one part of its business that acts as the ''supplier,'' and additional detail is needed about the relationship of the ''supplier component'' of the company to the rest of the business. Similarly, another commenter asserted that drug, biologics, and device manufacturers should not be covered entities simply by virtue of their manufacturing activities.

Response: We clarify that if a supplier manufacturer is a Medicare supplier, then it is a health care provider, and it is a covered entity if it conducts standard transactions. Further, we clarify that a manufacturer of supplies related to the health of a particular individual, e.g., prosthetic devices, is a health care provider because the manufacturer is providing ''health care'' as defined in the rule. However, that manufacturer is a covered entity only if it conducts standard transactions. We do not intend that a manufacturer of supplies that are generic and not customized or otherwise specifically designed for particular individuals, e.g., ace bandages for a hospital, is a health care provider. Such a manufacturer is not providing ''health care'' as defined in the rule and is therefore not a covered entity. We note that, even if such a manufacturer is a covered entity, it may be an ''indirect treatment provider'' under this rule, and thus not subject to all of the rule's requirements.

With regard to a ''supplier component,'' the final rule addresses the status of the unit or unit(s) of a larger entity that constitute a ''health care component.'' See further discussion under § 164.504 of this preamble.

Finally, we clarify that drug, biologics, and device manufacturers are not health care providers simply by virtue of their manufacturing activities. The manufacturer must be providing health care consistent with the final

rule's definition in order to be considered a health care provider.

Comment: A few commenters asked that the Department clarify that pharmaceutical manufacturers are not covered entities. It was explained that pharmaceutical manufacturers provide support and guidance to doctors and patients with respect to the proper use of their products, provide free products for doctors to distribute to patients, and operate charitable programs that provide pharmaceutical drugs to patients who cannot afford to buy the drugs they need.

Response: A pharmaceutical manufacturer is only a covered entity if the manufacturer provides ''health care'' according to the rule's definition and conducts standard transactions. In the above case, a pharmaceutical manufacturer that provides support and guidance to doctors and patients regarding the proper use of their products is providing ''health care'' for the purposes of this rule, and therefore, is a health care provider to the extent that it provides such services. The pharmaceutical manufacturer that is a health care provider is only a covered entity, however, if it conducts standard transactions. We note that this rule permits a covered entity to disclose protected health information to any person for treatment purposes, without specific authorization from the individual. Therefore, a covered health care provider is permitted to disclose protected health information to a pharmaceutical manufacturer for treatment purposes. Providing free samples to a health care provider does not in itself constitute health care. For further analysis of pharmacy assistance programs, see response to comment on § 164.501, definition of ''payment.''

Comment: Several commenters asked about the definition of ''covered entity'' and its application to health care entities within larger organizations.

Response: A detailed discussion of the final rule's organizational requirements and firewall restrictions for ''health care components'' of larger entities, as well as for affiliated, and other entities is found at the discussion of § 164.504 of this preamble. The following responses to comments provide additional information with respect to particular ''component entity'' circumstances.

Comment: Several commenters asked that we clarify the definition of covered entity to state that with respect to persons or organizations that provide health care or have created health plans but are primarily engaged in other unrelated businesses, the term ''covered entity'' encompasses only the health care components of the entity. Similarly, others recommended that only the component of a government agency that is a provider, health plan, or clearinghouse should be considered a covered entity.

Other commenters requested that we revise proposed § 160.102 to apply only to the component of an entity that engages in the transactions specified in the rule. Commenters stated that companies should remain free to employ licensed health care providers and to enter into corporate relationships with provider institutions without fear of being considered to be a covered entity. Another commenter suggested that the regulation not apply to the provider-employee or employer when neither the provider nor the company are a covered entity.

Some commenters specifically argued that the definition of ''covered entity'' did not contemplate an integrated health care system and one commenter stated that the proposal would disrupt the multi-disciplinary, collaborative approach that many take to health care today by treating all components as separate entities. Commenters, therefore, recommended that the rule treat the integrated entity, not its constituent parts, as the covered entity.

A few commenters asked that the Department further clarify the definition with respect to the unique organizational models and relationships of academic medical centers and their parent universities and the rules that govern information exchange within the institution. One commenter asked whether faculty physicians who are paid by a medical school or faculty practice plan and who are on the medical staff of, but not paid directly by, a hospital are included within the covered entity. Another commenter stated that it appears that only the health center at an academic institution is the covered entity. Uncertainty was also expressed as to whether other components of the institution that might create protected health information only incidentally through the conduct of research would also be covered.

Response: The Department understands that in today's health care industry, the relationships among health care entities and non-health care organizations are highly complex and varied. Accordingly, the final rule gives covered entities some flexibility to segregate or aggregate its operations for purposes of the application of this rule. The new component entity provision can be found at §§ 164.504(b)-(c). In response to the request for clarification on whether the rule would apply to a research component of the covered entity, we point out that if the research activities fall outside of the health care component they would not be subject to the rule. One organization may have one or several ''health care component(s)'' that each perform one or more of the health care functions of a covered entity, i.e., health care provider, health plan, health care clearinghouse. In addition, the final rule permits covered entities that are affiliated, *i.e.,* share common ownership or control, to designate themselves, or their health care components, together to be a single covered entity for purposes of the rule.

It appears from the comments that there is not a common understanding of the meaning of ''integrated delivery system.'' Arrangements that apply this label to themselves operate and share information many different ways, and may or may not be financially or clinically integrated. In some cases, multiple entities hold themselves out as one enterprise and engage together in clinical or financial activities. In others, separate entities share information but do not provide treatment together or share financial risk. Many health care providers participate in more than one such arrangement.

Therefore, we do not include a separate category of ''covered entity'' under this rule for ''integrated delivery systems'' but instead accommodate the operations of these varied arrangements through the functional provisions of the rule. For example, covered entities that operate as ''organized health care arrangements'' as defined in this rule may share protected health information for the operation of such arrangement without becoming business associates of one another. Similarly, the regulation does not require a business associate arrangement when protected health information is shared for purposes of providing treatment. The application of this rule to any particular ''integrated system'' will depend on the nature of the common activities the participants in the system perform. When the participants in such an arrangement are ''affiliated'' as defined in this rule, they may consider themselves a single covered entity (see § 164. 504).

The arrangements between academic health centers, faculty practice plans, universities, and hospitals are similarly diverse. We cannot describe a blanket rule that covers all such arrangements. The application of this rule will depend on the purposes for which the participants in such arrangements share protected health information, whether some or all participants are under common ownership or control, and similar matters. We note that physicians who have staff privileges at a covered

hospital do not become part of that hospital covered entity by virtue of having such privileges.

We reject the recommendation to apply the rule only to components of an entity that engage in the transactions. This would omit as covered entities, for example, the health plan components that do not directly engage in the transactions, including components that engage in important health plan functions such as coverage determinations and quality review. Indeed, we do not believe that the statute permits this result with respect to health plans or health care clearinghouses as a matter of negative implication from section 1172(a)(3). We clarify that only a health care provider must conduct transactions to be a covered entity for purposes of this rule.

We also clarify that health care providers (such as doctors or nurses) who work for a larger organization and do not conduct transactions on their own behalf are workforce members of the covered entity, not covered entities themselves.

Comment: A few commenters asked the Department to clarify the definition to provide that a multi-line insurer that sells insurance coverages, some of which do and others which do not meet the definition of ''health plan,'' is not a covered entity with respect to actions taken in connection with coverages that are not ''health plans.''

Response: The final rule clarifies that the requirements below apply only to the organizational unit or units of the organization that are the ''health care component'' of a covered entity, where the ''covered functions'' are not the primary functions of the entity. Therefore, for a multi-line insurer, the ''health care component'' is the insurance line(s) that conduct, or support the conduct of, the health care function of the covered entity. Also, it should be noted that excepted benefits, such as life insurance, are not included in the definition of ''health plan.'' (See preamble discussion of § 164.504).

Comment: A commenter questioned whether the Health Care Financing Administration (HCFA) is a covered entity and how HCFA will share data with Medicare managed care organizations. The commenter also questioned why the regulation must apply to Medicaid since the existing Medicaid statute requires that states have privacy standards in place. It was also requested that the Department provide a definition of ''health plan'' to clarify that state Medicaid Programs are considered as such.

Response: HCFA is a covered entity because it administers Medicare and Medicaid, which are both listed in the statute as health plans. Medicare managed care organizations are also covered entities under this regulation. As noted elsewhere in this preamble, covered entities that jointly administer a health plan, such as Medicare + Choice, are both covered entities, and are not business associates of each other by virtue of such joint administration.

We do not exclude state Medicaid programs. Congress explicitly included the Medicaid program as a covered health plan in the HIPAA statute.

Comment: A commenter asked the Department to provide detailed guidance as to when providers, plans, and clearinghouses become covered entities. The commenter provided the following example: if a provider submits claims only in paper form, and a coordination of benefits (COB) transaction is created due to other insurance coverage, will the original provider need to be notified that the claim is now in electronic form, and that it has become a covered entity? Another commenter voiced concern as to whether physicians who do not conduct electronic transactions would become covered entities if another entity using its records downstream transmits information in connection with a standard transaction on their behalf.

Response: We clarify that health care providers who submit the transactions in standard electronic form, health plans, and health care clearinghouses are covered entities if they meet the respective definitions. Health care providers become subject to the rule if they conduct standard transactions. In the above example, the health care provider would not be a covered entity if the coordination of benefits transaction was generated by a payor.

We also clarify that health care providers who do not submit transactions in standard form become covered by this rule when other entities, such as a billing service or a hospital, transmit standard electronic transactions on the providers' behalf. However, where the downstream transaction is not conducted on behalf of the health care provider, the provider does not become a covered entity due to the downstream transaction.

Comment: Several commenters discussed the relationship between section 1179 of the Act and the privacy regulations. One commenter suggested that HHS retain the statement that a covered entity means ''the entities to which part C of title XI of the Act applies.'' In particular, the commenter observed that section 1179 of the Act provides that part C of title XI of the Act does not apply to financial institutions or to entities acting on behalf of such institutions that are covered by the section 1179 exemption. Thus, under the definition of covered entity, they comment that financial institutions and other entities that come within the scope of the section 1179 exemption are appropriately not covered entities.

Other commenters maintained that section 1179 of the Act means that the Act's privacy requirements do not apply to the request for, or the use or disclosure of, information by a covered entity with respect to payment: (a) For transferring receivables; (b) for auditing; (c) in connection with—(i) a customer dispute; or (ii) an inquiry from or to a customer; (d) in a communication to a customer of the entity regarding the customer's transactions payment card, account, check, or electronic funds transfer; (e) for reporting to consumer reporting agencies; or (f) for complying with: (i) a civil or criminal subpoena; or (ii) a federal or state law regulating the entity. These companies expressed concern that the proposed rule did not include the full text of section 1179 when discussing the list of activities that were exempt from the rule's requirements. Accordingly, they recommended including in the final rule either a full listing of or a reference to section 1179's full list of exemptions. Furthermore, these firms opposed applying the proposed rule's minimum necessary standard for disclosure of protected health information to financial institutions because of section 1179.

These commenters suggest that in light of section 1179, HHS lacks the authority to impose restrictions on financial institutions and other entities when they engage in activities described in that section. One commenter expressed concern that even though proposed § 164.510(i) would have permitted covered entities to disclose certain information to financial institutions for banking and payment processes, it did not state clearly that financial institutions and other entities described in section 1179 are exempt from the rule's requirements.

Response: We interpret section 1179 of the Act to mean that entities engaged in the activities of a financial institution, and those acting on behalf of a financial institution, are not subject to this regulation when they are engaged in authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments for a financial institution. The statutory reference to 12 U.S.C. 3401 indicates that Congress chose to adopt the definition of financial institutions found

in the Right to Financial Privacy Act, which defines financial institutions as any office of a bank, savings bank, card issuer, industrial loan company, trust company, savings association, building and loan, homestead association, cooperative bank, credit union, or consumer finance institution located in the United States or one of its Territories. Thus, when we use the term ''financial institution'' in this regulation, we turn to the definition with which Congress provided us. We interpret this provision to mean that when a financial institution, or its agent on behalf of the financial institution, conducts the activities described in section 1179, the privacy regulation will not govern the activity.

If, however, these activities are performed by a covered entity or by another entity, including a financial institution, on behalf of a covered entity, the activities are subject to this rule. For example, if a bank operates the accounts payable system or other ''back office'' functions for a covered health care provider, that activity is not described in section 1179. In such instances, because the bank would meet the rule's definition of ''business associate,'' the provider must enter into a business associate contract with the bank before disclosing protected health information pursuant to this relationship. However, if the same provider maintains an account through which he/she cashes checks from patients, no business associate contract would be necessary because the bank's activities are not undertaken for or on behalf of the covered entity, and fall within the scope of section 1179. In part to give effect to section 1179, in this rule we do not consider a financial institution to be acting on behalf of a covered entity when it processes consumer-conducted financial transactions by debit, credit or other payment card, clears checks, initiates or processes electronic funds transfers, or conducts any other activity that directly facilitates or effects the transfer of funds for compensation for health care.

We do not agree with the comment that section 1179 of the Act means that the privacy regulation's requirements cannot apply to the activities listed in that section; rather, it means that the entities expressly mentioned, financial institutions (as defined in the Right to Financial Privacy Act), and their agents that engage in the listed activities for the financial institution are not within the scope of the regulation. Nor do we interpret section 1179 to support an exemption for disclosures to financial institutions from the minimum necessary provisions of this regulation.

Comment: One commenter recommended that HHS include a definition of ''entity'' in the final rule because HIPAA did not define it. The commenter explained that in a modern health care environment, the organization acting as the health plan or health care provider may involve many interrelated corporate entities and that this could lead to difficulties in determining what ''entities'' are actually subject to the regulation.

Response: We reject the commenter's suggestion. We believe it is clear in the final rule that the entities subject to the regulation are those listed at § 160.102. However, we acknowledge that how the rule applies to integrated or other complex health systems needs to be addressed; we have done so in § 164.504 and in other provisions, such as those addressing organized health care arrangements.

Comment: The preamble should clarify that self-insured group health and workmen's compensation plans are not covered entities or business partners.

Response: In the preamble to the proposed rule we stated that certain types of insurance entities, such as workers' compensation, would not be covered entities under the rule. We do not change this position in this final rule. The statutory definition of health plan does not include workers' compensation products, and the regulatory definition of the term specifically excludes them. However, HIPAA specifically includes most group health plans within the definition of ''health plan.''

Comment: A health insurance issuer asserted that health insurers and third party administrators are usually required by employers to submit reports describing the volume, amount, payee, basis for services rendered, types of claims paid and services for which payment was requested on behalf of it covered employees. They recommended that the rule permit the disclosure of protected health information for such purposes.

Response: We agree that health plans should be able to disclose protected health information to employers sponsoring health plans under certain circumstances. Section 164.504(f) explains the conditions under which protected health information may be disclosed to plan sponsors. We believe that this provision gives sponsors access to the information they need, but protects individual's information to the extent possible under our legislative authority.

Group Health Plan

For response to comments relating to ''group health plan,'' see the response to comments on ''health plan'' below and the response to comments on § 164.504.

Health Care

Comment: A number of commenters asked that we include disease management activities and other similar health improvement programs, such as preventive medicine, health education services and maintenance, health and case management, and risk assessment, in the definition of ''health care.'' Commenters maintained that the rule should avoid limiting technological advances and new health care trends intended to improve patient ''health care.''

Response: Review of these and other comments, and our fact-finding, indicate that there are multiple, different, understandings of the definition of these terms. Therefore, rather than create a blanket rule that includes such terms in or excludes such terms from the definition of ''health care,'' we define health care based on the underlying activities that constitute health care. The activities described by these commenters are considered ''health care'' under this rule to the extent that they meet this functional definition. Listing activities by label or title would create the risk that important activities would be left out and, given the lack of consensus on what these terms mean, could also create confusion.

Comment: Several commenters urged that the Department clarify that the activities necessary to procure and distribute eyes and eye tissue will not be hampered by the rule. Some of these commenters explicitly requested that we include ''eyes and eye tissue'' in the list of procurement biologicals as well as ''eye procurement'' in the definition of ''health care.'' In addition, it was argued that ''administration to patients'' be excluded in the absence of a clear definition. Also, commenters recommended that the definition include other activities associated with the transplantation of organs, such as processing, screening, and distribution.

Response: We delete from the definition of ''health care'' activities related to the procurement or banking of blood, sperm, organs, or any other tissue for administration to patients. We do so because persons who make such donations are not seeking to be treated, diagnosed, or assessed or otherwise seeking health care for themselves, but are seeking to contribute to the health care of others. In addition, the nature of

these activities entails a unique kind of information sharing and tracking necessary to safeguard the nation's organ and blood supply, and those seeking to donate are aware that this information sharing will occur. Consequently, such procurement or banking activities are not considered health care and the organizations that perform such activities are not considered health care providers for purposes of this rule.

With respect to disclosure of protected health information by covered entities to facilitate cadaveric organ and tissue donation, the final rule explicitly permits a covered entity to disclose protected health information without authorization, consent, or agreement to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating donation and transplantation. See § 164.512(h). We do not include blood or sperm banking in this provision because, for those activities, there is direct contact with the donor, and thus opportunity to obtain the individual's authorization.

Comment: A large number of commenters urged that the term ''assessment'' be included in the list of services in the definition, as ''assessment'' is used to determine the baseline health status of an individual. It was explained that assessments are conducted in the initial step of diagnosis and treatment of a patient. If assessment is not included in the list of services, they pointed out that the services provided by occupational health nurses and employee health information may not be covered.

Response: We agree and have added the term ''assessment'' to the definition to clarify that this activity is considered ''health care'' for the purposes of the rule.

Comment: One commenter asked that we revise the definition to explicitly exclude plasmapheresis from paragraph (3) of the definition. It was explained that plasmapheresis centers do not have direct access to health care recipients or their health information, and that the limited health information collected about plasma donors is not used to provide health care services as indicated by the definition of health care.

Response: We address the commenters' concerns by removing the provision related to procurement and banking of human products from the definition.

Health Care Clearinghouse

Comment: The largest set of comments relating to health care clearinghouses focused on our proposal to exempt health care clearinghouses from the patient notice and access rights provisions of the regulation. In our NPRM, we proposed to exempt health care clearinghouses from certain provisions of the regulation that deal with the covered entities' notice of information practices and consumers' rights to inspect, copy, and amend their records. The rationale for this exemption was based on our belief that health care clearinghouses engage primarily in business-to-business transactions and do not initiate or maintain direct relationships with individuals. We proposed this position with the caveat that the exemptions would be void for any health care clearinghouse that had direct contact with individuals in a capacity other than that of a business partner. In addition, we indicated that, in most instances, clearinghouses also would be considered business partners under this rule and would be bound by their contracts with covered plans and providers. They also would be subject to the notice of information practices developed by the plans and providers with whom they contract.

Commenters stated that, although health care clearinghouses do not have direct contact with individuals, they do have individually identifiable health information that may be subject to misuse or inappropriate disclosure. They expressed concern that we were proposing to exempt health care clearinghouses from all or many aspects of the regulation. These commenters suggested that we either delete the exemption or make it very narrow, specific and explicit in the final regulatory text.

Clearinghouse commenters, on the other hand, were in agreement with our proposal, including the exemption provision and the provision that the exemption is voided when the entity does have direct contact with individuals. They also stated that a health care clearinghouse that has a direct contact with individuals is no longer a health care clearinghouse as defined and should be subject to all requirements of the regulation.

Response: In the final rule, where a clearinghouse creates or receives protected health information as a business associate of another covered entity, we maintain the exemption for health care clearinghouses from certain provisions of the regulation dealing with the notice of information practices and patient's direct access rights to inspect, copy and amend records (§§ 164.524 and 164.526), on the grounds that a health care clearinghouse is engaged in business-to-business operations, and is not dealing directly with individuals. Moreover, as business associates of plans and providers, health care clearinghouses are bound by the notices of information practices of the covered entities with whom they contract.

Where a health care clearinghouse creates or receives protected health information other than as a business associate, however, it must comply with all the standards, requirements, and implementation specifications of the rule. We describe and delimit the exact nature of the exemption in the regulatory text. See § 164.500(b). We will monitor developments in this sector should the basic business-to-business relationship change.

Comment: A number of comments relate to the proposed definition of health care clearinghouse. Many commenters suggested that we expand the definition. They suggested that additional types of entities be included in the definition of health care clearinghouse, specifically medical transcription services, billing services, coding services, and ''intermediaries.'' One commenter suggested that the definition be expanded to add entities that receive standard transactions, process them and clean them up, and then send them on, without converting them to any standard format. Another commenter suggested that the health care clearinghouse definition be expanded to include entities that do not perform translation but may receive protected health information in a standard format and have access to that information. Another commenter stated that the list of covered entities should include any organization that receives or maintains individually identifiable health information. One organization recommended that we expand the health care clearinghouse definition to include the concept of a research data clearinghouse, which would collect individually identifiable health information from other covered entities to generate research data files for release as de-identified data or with appropriate confidentiality safeguards. One commenter stated that HHS had gone beyond Congressional intent by including billing services in the definition.

Response: We cannot expand the definition of ''health care clearinghouse'' to cover entities not covered by the definition of this term in the statute. In the final regulation, we

make a number of changes to address public comments relating to definition. We modify the definition of health care clearinghouse to conform to the definition published in the Transactions Rule (with the addition of a few words, as noted above). We clarify in the preamble that, while the term ''health care clearinghouse'' may have other meanings and connotations in other contexts, for purposes of this regulation an entity is considered a health care clearinghouse only to the extent that it actually meets the criteria in our definition. Entities performing other functions but not meeting the criteria for a health care clearinghouse are not clearinghouses, although they may be business associates. Billing services are included in the regulatory definition of ''health care clearinghouse,'' if they perform the specified clearinghouse functions. Although we have not added or deleted any entities from our original definition, we will monitor industry practices and may add other entities in the future as changes occur in the health system.

Comment: Several commenters suggested that we clarify that an entity acting solely as a conduit through which individually identifiable health information is transmitted or through which protected health information flows but is not stored is not a covered entity, e.g., a telephone company or Internet Service Provider. Other commenters indicated that once a transaction leaves a provider or plan electronically, it may flow through several entities before reaching a clearinghouse. They asked that the regulation protect the information in that interim stage, just as the security NPRM established a chain of trust arrangement for such a network. Others noted that these ''conduit'' entities are likely to be business partners of the provider, clearinghouse or plan, and we should clarify that they are subject to business partner obligations as in the proposed Security Rule.

Response: We clarify that entities acting as simple and routine communications conduits and carriers of information, such as telephone companies and Internet Service Providers, are not clearinghouses as defined in the rule unless they carry out the functions outlined in our definition. Similarly, we clarify that value added networks and switches are not health care clearinghouses unless they carry out the functions outlined in the definition, and clarify that such entities may be business associates if they meet the definition in the regulation.

Comment: Several commenters, including the large clearinghouses and their trade associations, suggested that we not treat health care clearinghouses as playing a dual role as covered entity and business partner in the final rule because such a dual role causes confusion as to which rules actually apply to clearinghouses. In their view, the definition of health care clearinghouse is sufficiently clear to stand alone and identify a health care clearinghouse as a covered entity, and allows health care clearinghouses to operate under one consistent set of rules.

Response: For reasons explained in § 164.504 of this preamble, we do not create an exception to the business associate requirements when the business associate is also a covered entity. We retain the concept that a health care clearinghouse may be a covered entity and a business associate of a covered entity under the regulation. As business associates, they would be bound by their contracts with covered plans and providers.

Health Care Provider

Comment: One commenter pointed out that the preamble referred to the obligations of providers and did not use the term, ''covered entity,'' and thus created ambiguity about the obligations of health care providers who may be employed by persons other than covered entities, e.g., pharmaceutical companies. It was suggested that a better reading of the statute and rule is that where neither the provider nor the company is a covered entity, the rule does not impose an obligation on either the provider-employee or the employer.

Response: We agree. We use the term ''covered entity'' whenever possible in the final rule, except for the instances where the final rule treats the entities differently, or where use of the term ''health care provider'' is necessary for purposes of illustrating an example.

Comment: Several commenters stated that the proposal's definition was broad, unclear, and/or confusing. Further, we received many comments requesting clarification as to whether specific entities or persons were ''health care providers'' for the purposes of our rule. One commenter questioned whether affiliated members of a health care group (even though separate legal entities) would be considered as one primary health care provider.

Response: We permit legally distinct covered entities that share common ownership or control to designate themselves together to be a single covered entity. Such organizations may promulgate a single shared notice of information practices and a consent form. For more detailed information, see the preamble discussion of § 164.504(d).

We understand the need for additional guidance on whether specific entities or persons are health care providers under the final rule. We provide guidance below and will provide additional guidance as the rule is implemented.

Comment: One commenter observed that sections 1171(3), 1861(s) and 1861(u) of the Act do not include pharmacists in the definition of health care provider or pharmacist services in the definition of ''medical or other health services,'' and questioned whether pharmacists were covered by the rule.

Response: The statutory definition of ''health care provider'' at section 1171(3) includes ''any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.'' Pharmacists' services are clearly within this statutory definition of ''health care.'' There is no basis for excluding pharmacists who meet these statutory criteria from this regulation.

Comment: Some commenters recommended that the scope of the definition be broadened or clarified to cover additional persons or organizations. Several commenters argued for expanding the reach of the health care provider definition to cover entities such as state and local public health agencies, maternity support services (provided by nutritionists, social workers, and public health nurses and the Special Supplemental Nutrition Program for Women, Infants and Children), and those companies that conduct cost-effectiveness reviews, risk management, and benchmarking studies. One commenter queried whether auxiliary providers such as child play therapists, and speech and language therapists are considered to be health care providers. Other commenters questioned whether ''alternative'' or ''complementary'' providers, such as naturopathic physicians and acupuncturists would be considered health care providers covered by the rule.

Response: As with other aspects of this rule, we do not define ''health care provider'' based on the title or label of the professional. The professional activities of these kinds of providers vary; a person is a ''health care provider'' if those activities are consistent with the rule's definition of ''health care provider.'' Thus, health care providers include persons, such as those noted by the commenters, to the extent that they meet the definition. We note that health care providers are only

subject to this rule if they conduct certain transactions. See the definition of ''covered entity.''

However companies that conduct cost-effectiveness reviews, risk management, and benchmarking studies are not health care providers for the purposes of this rule unless they perform other functions that meet the definition. These entities would be business associates if they perform such activities on behalf of a covered entity.

Comment: Another commenter recommended that the Secretary expand the definition of health care provider to cover health care providers who transmit or ''or receive'' any health care information in electronic form.

Response: We do not accept this suggestion. Section 1172(a)(3) states that providers that ''transmit'' health information in connection with one of the HIPAA transactions are covered, but does not use the term ''receive'' or a similar term.

Comment: Some comments related to online companies as health care providers and covered entities. One commenter argued that there was no reason ''why an Internet pharmacy should not also be covered'' by the rule as a health care provider. Another commenter stated that online health care service and content companies, including online medical record companies, should be covered by the definition of health care provider. Another commenter pointed out that the definitions of covered entities cover ''Internet providers who 'bill' or are 'paid' for health care services or supplies, but not those who finance those services in other ways, such as through sale of identifiable health information or advertising.'' It was pointed out that thousands of Internet sites use information provided by individuals who access the sites for marketing or other purposes.

Response: We agree that online companies are covered entities under the rule if they otherwise meet the definition of health care provider or health plan and satisfy the other requirements of the rule, i.e., providers must also transmit health information in electronic form in connection with a HIPAA transaction. We restate here the language in the preamble to the proposed rule that ''An individual or organization that bills and/or is paid for health care services or supplies in the normal course of business, such as * * * an ''online'' pharmacy accessible on the Internet, is also a health care provider for purposes of this statute'' (64 FR 59930).

Comment: We received many comments related to the reference to ''health clinic or licensed health care professional located at a school or business in the preamble's discussion of ''health care provider.'' It was stated that including ''licensed health care professionals located at a school or business'' highlights the need for these individuals to understand they have the authority to disclose information to the Social Security Administration (SSA) without authorization.

However, several commenters urged HHS to create an exception for or delete that reference in the preamble discussion to primary and secondary schools because of employer or business partner relationships. One federal agency suggested that the reference ''licensed health care professionals located at a [school]'' be deleted from the preamble because the definition of health care provider does not include a reference to schools. The commenter also suggested that the Secretary consider: adding language to the preamble to clarify that the rules do not apply to clinics or school health care providers that only maintain records that have been excepted from the definition of protected health information, adding an exception to the definition of covered entities for those schools, and limiting paperwork requirements for these schools. Another commenter argued for deleting references to schools because the proposed rule appeared to supersede or create ambiguity as to the Family Educational Rights and Privacy Act (FERPA), which gives parents the right to access ''education'' and health records of their unemancipated minor children. However, in contrast, one commenter supported the inclusion of health care professionals who provide services at schools or businesses.

Response: We realize that our discussion of schools in the NPRM may have been confusing. Therefore, we address these concerns and set forth our policy regarding protected health information in educational agencies and institutions in the ''Relationship to Other Federal Laws'' discussion of FERPA, above.

Comment: Many commenters urged that direct contact with the patient be necessary for an entity to be considered a health care provider. Commenters suggested that persons and organizations that are remote to the patient and have no direct contact should not be considered health care providers. Several commenters argued that the definition of health care provider covers a person that provides health care services or supplies only when the provider furnishes to or bills the patient directly. It was stated that the Secretary did not intend that manufacturers, such as pharmaceutical, biologics, and device manufacturers, health care suppliers, medical-surgical supply distributors, health care vendors that offer medical record documentation templates and that typically do not deal directly with the patient, be considered health care providers and thus covered entities. However, in contrast, one commenter argued that, as an in vitro diagnostics manufacturer, it should be covered as a health care provider.

Response: We disagree with the comments that urged that direct dealings with an individual be a prerequisite to meeting the definition of health care provider. Many providers included in the statutory definition of provider, such as clinical labs, do not have direct contact with patients. Further, the use and disclosure of protected health information by indirect treatment providers can have a significant effect on individuals' privacy. We acknowledge, however, that providers who treat patients only indirectly need not have the full array of responsibilities as direct treatment providers, and modify the NPRM to make this distinction with respect to several provisions (see, for example § 164.506 regarding consent). We also clarify that manufacturers and health care suppliers who are considered providers by Medicare are providers under this rule.

Comment: Some commenters suggested that blood centers and plasma donor centers that collect and distribute source plasma not be considered covered health care providers because the centers do not provide ''health care services'' and the blood donors are not ''patients'' seeking health care. Similarly, commenters expressed concern that organ procurement organizations might be considered health care providers.

Response: We agree and have deleted from the definition of ''health care'' the term ''procurement or banking of blood, sperm, organs, or any other tissue for administration to patients.'' See prior discussion under ''health care.''

Comment: Several commenters proposed to restrict coverage to only those providers who furnished and were paid for services and supplies. It was argued that a salaried employee of a covered entity, such as a hospital-based provider, should not be covered by the rule because that provider would be subject both directly to the rule as a covered entity and indirectly as an employee of a covered entity.

Response: The ''dual'' direct and indirect situation described in these comments can arise only when a health

care provider conducts standard HIPAA transactions both for itself and for its employer. For example, when the services of a provider such as a hospital-based physician are billed through a standard HIPAA transaction conducted for the employer, in this example the hospital, the physician does not become a covered provider. Only when the provider uses a standard transaction on its own behalf does he or she become a covered health care provider. Thus, the result is typically as suggested by this commenter. When a hospital-based provider is not paid directly, that is, when the standard HIPAA transaction is not on its behalf, it will not become a covered provider.

Comment: Other commenters argued that an employer who provides health care services to its employees for whom it neither bills the employee nor pays for the health care should not be considered health care providers covered by the proposed rule.

Response: We clarify that the employer may be a health care provider under the rule, and may be covered by the rule if it conducts standard transactions. The provisions of § 164.504 may also apply.

Comment: Some commenters were confused about the preamble statement: ''in order to implement the principles in the Secretary's Recommendations, we must impose any protections on the health care providers that use and disclose the information, rather than on the researcher seeking the information,'' with respect to the rule's policy that a researcher who provides care to subjects in a trial will be considered a health care provider. Some commenters were also unclear about whether the individual researcher providing health care to subjects in a trial would be considered a health care provider or whether the researcher's home institution would be considered a health care provider and thus subject to the rule.

Response: We clarify that, in general, a researcher is also a health care provider if the researcher provides health care to subjects in a clinical research study and otherwise meets the definition of ''health care provider'' under the rule. However, a health care provider is only a covered entity and subject to the rule if that provider conducts standard transactions. With respect to the above preamble statement, we meant that our jurisdiction under the statute is limited to covered entities. Therefore, we cannot apply any restrictions or requirements on a researcher in that person's role as a researcher. However, if a researcher is also a health care provider that conducts standard transactions, that researcher/provider is subject to the rule with regard to its provider activities.

As to applicability to a researcher/provider versus the researcher's home institution, we provide the following guidance. The rule applies to the researcher as a covered entity if the researcher is a health care provider who conducts standard transactions for services on his or her own behalf, regardless of whether he or she is part of a larger organization. However, if the services and transactions are conducted on behalf of the home institution, then the home institution is the covered entity for purposes of the rule and the researcher/provider is a workforce member, not a covered entity.

Comment: One commenter expressed confusion about those instances when a health care provider was a covered entity one day, and one who ''works under a contract'' for a manufacturer the next day.

Response: If persons are covered under the rule in one role, they are not necessarily covered entities when they participate in other activities in another role. For example, that person could be a covered health care provider in a hospital one day but the next day read research records for a different employer. In its role as researcher, the person is not covered, and protections do not apply to those research records.

Comment: One commenter suggested that the Secretary modify proposed § 160.102, to add the following clause at the end (after (c)) (regarding health care provider), ''With respect to any entity whose *primary* business is not that of a health plan or health care provider licensed under the applicable laws of any state, the standards, requirements, and implementation specifications of this subchapter shall apply solely to the component of the entity that engages in the transactions specified in [§] 160.103.'' (Emphasis added.) Another commenter also suggested that the definition of ''covered entity'' be revised to mean entities that are ''primarily or exclusively engaged in health care-related activities as a health plan, health care provider, or health care clearinghouse.''

Response: The Secretary rejects these suggestions because they will impermissibly limit the entities covered by the rule. An entity that is a health plan, health care provider, or health care clearinghouse meets the statutory definition of covered entity regardless of how much time is devoted to carrying out health care-related functions, or regardless of what percentage of their total business applies to health care-related functions.

Comment: Several commenters sought to distinguish a health care provider from a business partner as proposed in the NPRM. For example, a number of commenters argued that disease managers that provide services ''on behalf of'' health plans and health care providers, and case managers (a variation of a disease management service) are business partners and not ''health care providers.'' Another commenter argued that a disease manager should be recognized (presumably as a covered entity) because of its involvement from the physician-patient level through complex interactions with health care providers.

Response: To the extent that a disease or case manager provides services on behalf of or to a covered entity as described in the rule's definition of business associate, the disease or case manager is a business associate for purposes of this rule. However, if services provided by the disease or case manager meet the definition of treatment and the person otherwise meets the definition of ''health care provider,'' such a person is a health care provider for purposes of this rule.

Comment: One commenter argued that pharmacy employees who assist pharmacists, such as technicians and cashiers, are not business partners.

Response: We agree. Employees of a pharmacy that is a covered entity are workforce members of that covered entity for purposes of this rule.

Comment: A number of commenters requested that we clarify the definition of health care provider (''* * * who furnishes, bills, or is paid for health care services or supplies in the normal course of business'') by defining the various terms ''furnish'', ''supply'', and ''in the normal course of business.'' For instance, it was stated that this would help employers recognize when services such as an employee assistance program constituted health care covered by the rule.

Response: Although we understand the concern expressed by the commenters, we decline to follow their suggestion to define terms at this level of specificity. These terms are in common use today, and an attempt at specific definition would risk the inadvertent creations of conflict with industry practices. There is a significant variation in the way employers structure their employee assistance programs (EAPs) and the type of services that they provide. If the EAP provides direct treatment to individuals, it may be a health care provider.

Health Information

The response to comments on health information is included in the response to comments on individually identifiable health information, in the preamble discussion of § 164.501.

Health Plan

Comment: One commenter suggested that to eliminate any ambiguity, the Secretary should clarify that the catch-all category under the definition of health plan includes ''24-hour coverage plans'' (whether insured or self-insured) that integrate traditional employee health benefits coverage and workers' compensation coverage for the treatment of on-the-job injuries and illnesses under one program. It was stated that this clarification was essential if the Secretary persisted in excluding workers' compensation from the final rule.

Response: We understand concerns that such plans may use and disclose individually identifiable health information. We therefore clarify that to the extent that 24-hour coverage plans have a health care component that meets the definition of ''health plan'' in the final rule, such components must abide by the provisions of the final rule. In the final rule, we have added a new provision to § 164.512 that permits covered entities to disclose information under workers' compensation and similar laws. A health plan that is a 24-hour plan is permitted to make disclosures as necessary to comply with such laws.

Comment: A number of commenters urged that certain types of insurance entities, such as workers' compensation and automobile insurance carriers, property and casualty insurance health plans, and certain forms of limited benefits coverage, be included in the definition of ''health plan.'' It was argued that consumers deserve the same protection with respect to their health information, regardless of the entity using it, and that it would be inequitable to subject health insurance carriers to more stringent standards than other types of insurers that use individually identifiable health information.

Response: The Congress did not include these programs in the definition of a ''health plan'' under section 1171 of the Act. Further, HIPAA's legislative history shows that the House Report's (H. Rep. 104–496) definition of ''health plan'' originally included certain benefit programs, such as workers' compensation and liability insurance, but was later amended to clarify the definition and remove these programs. Thus, since the statutory definition of a health plan both on its face and through legislative history evidence Congress' intention to exclude such programs, we do not have the authority to require that these programs comply with the standards. We have added explicit language to the final rule which excludes the excepted benefit programs, as defined in section 2971(c)(1) of the PHS Act, 42 U.S.C. 300gg-91(c)(1).

Comment: Some commenters urged HHS to include entities such as stop loss insurers and reinsurers in the definition of ''health plan.'' It was observed that such entities have come to play important roles in managed care delivery systems. They asserted that increasingly, capitated health plans and providers contract with their reinsurers and stop loss carriers to medically manage their high cost outlier cases such as organ and bone marrow transplants, and therefore should be specifically cited as subject to the regulations.

Response: Stop-loss and reinsurers do not meet the statutory definition of health plan. They do not provide or pay for the costs of medical care, as described in the statute, but rather insure health plans and providers against unexpected losses. Therefore, we cannot include them as health plans in the regulation.

Comment: A commenter asserted that there is a significant discrepancy between the effect of the definition of ''group health plan'' as proposed in § 160.103, and the anticipated impact in the cost estimates of the proposed rule at 64 FR 60014. Paragraph (1) of the proposed definition of ''health plan'' defined a ''group health plan'' as an ERISA-defined employee welfare benefit plan that provides medical care and that: ''(i) Has 50 or more participants, *or* (ii) Is administered by an entity other than the employer that established and maintains the plan[.]'' (emphasis added) According to this commenter, under this definition, the only insured or self-insured ERISA plans that would not be regulated ''health plans'' would be those that have less than 50 participants and are self administered.

The commenter presumed that the we had intended to exclude from the definition of ''health plan'' (and from coverage under the proposed rule) all ERISA plans that are small (less than 50 participants) *or* are administered by a third party, whether large or small, based on the statement at 64 FR 60014, note 18. That footnote stated that the Department had ''not included the 3.9 million 'other' employer-health plans listed in HCFA's administrative simplification regulations because these plans are administered by a third party. The proposed regulation will not regulate the employer plans but will regulate the third party administrators of the plan.'' The commenter urged us not to repeat the statutory definition, and to adopt the policy implied in the footnote.

Response: We agree with the commenter's observation that footnote 18 (64 FR 60014) was inconsistent with the proposed definition. We erred in drafting that note. The definition of ''group health plan'' is adopted from the statutory definition at section 1171(5)(A), and excludes from the rule as ''health plans'' only the few insured or self-insured ERISA plans that have less than 50 participants *and* are self administered. We reject the commenter's proposed change to the definition as inconsistent with the statute.

Comment: A number of insurance companies asked that long term care insurance policies be excluded from the definition of ''health plan.'' It was argued that such policies do not provide sufficiently comprehensive coverage of the cost of medical care, and are limited benefit plans that provide or pay for the cost of custodial and other related services in connection with a long term, chronic illness or disability.

These commenters asserted that HIPAA recognizes this nature of long term care insurance, observing that, with respect to HIPAA's portability requirements, Congress enacted a series of exclusions for certain defined types of health plan arrangements that do not typically provide comprehensive coverage. They maintained that Congress recognized that long term care insurance is excluded, so long as it is not a part of a group health plan. Where a long term care policy is offered separately from a group health plan it is considered an excepted benefit and is not subject to the portability and guarantee issue requirements of HIPAA. Although this exception does not appear in the Administrative Simplification provisions of HIPAA, it was asserted that it is guidance with respect to the treatment of long term care insurance as a limited benefit coverage and not as coverage that is so ''sufficiently comprehensive'' that it is to be treated in the same manner as a typical, comprehensive major medical health plan arrangement.

Another commenter offered a different perspective observing that there are some long-term care policies—that do not pay for medical care and therefore are not ''health plans.'' It was noted that most long-term care policies are reimbursement policies—that is,

they reimburse the policyholder for the actual expenses that the insured incurs for long-term care services. To the extent that these constitute ''medical care,'' this commenter presumed that these policies would be considered ''health plans.'' Other long-term care policies, they pointed out, simply pay a fixed dollar amount when the insured becomes chronically ill, without regard to the actual cost of any long-term care services received, and thus are similar to fixed indemnity critical illness policies. The commenter suggested that while there was an important distinction between indemnity based long-term care policies and expenses based long-term care policies, it may be wise to exclude all long-term care policies from the scope of the rule to achieve consistency with HIPAA.

Response: We disagree. The statutory language regarding long-term care policies in the portability title of HIPAA is different from the statutory language regarding long-term care policies in the Administrative Simplification title of HIPAA. Section 1171(5)(G) of the Act means that issuers of long-term care policies are considered health plans for purposes of administrative simplification. We also interpret the statute as authorizing the Secretary to exclude nursing home fixed-indemnity policies, not all long-term care policies, from the definition of ''health plan,'' if she determines that these policies do not provide ''sufficiently comprehensive coverage of a benefit'' to be treated as a health plan (see section 1171 of the Act). We interpret the term ''comprehensive'' to refer to the breadth or scope of coverage of a policy. ''Comprehensive'' policies are those that cover a range of possible service options. Since nursing home fixed indemnity policies are, by their own terms, limited to payments made solely for nursing facility care, we have determined that they should not be included as health plans for the purposes of the HIPAA regulations. The Secretary, therefore, explicitly excluded nursing home fixed-indemnity policies from the definition of ''health plan'' in the Transactions Rule, and this exclusion is thus reflected in this final rule. Issuers of other long-term care policies are considered to be health plans under this rule and the Transactions Rule.

Comment: One commenter was concerned about the potential impact of the proposed regulations on ''unfunded health plans,'' which the commenter described as programs used by smaller companies to provide their associates with special employee discounts or other membership incentives so that they can obtain health care, including prescription drugs, at reduced prices. The commenter asserted that if these discount and membership incentive programs were covered by the regulation, many smaller employers might discontinue offering them to their employees, rather than deal with the administrative burdens and costs of complying with the rule.

Response: Only those special employee discounts or membership incentives that are ''employee welfare benefit plans'' as defined in section 3(1) of the Employee Retirement Income Security Act of 1974, 29 U.S.C. 1002(1), and provide ''medical care'' (as defined in section 2791(a)(2) of the Public Health Service Act, 42 U.S.C. 300gg-91(a)(2)), are health plans for the purposes of this rule. Discount or membership incentive programs that are not group health plans are not covered by the rule.

Comment: Several commenters agreed with the proposal to exclude ''excepted benefits'' such as disability income insurance policies, fixed indemnity critical illness policies, and per diem long-term care policies from the definition of ''health plan,'' but were concerned that the language of the proposed rule did not fully reflect this intent. They asserted that clarification was necessary in order to avoid confusion and costs to both consumers and insurers.

One commenter stated that, while HHS did not intend for the rule to apply to every type of insurance coverage that paid for medical care, the language of the proposed rule did not bear this out. The problem, it was asserted, is that under the proposed rule any insurance policy that pays for ''medical care'' would technically be a ''health plan.'' It was argued that despite the statements in the narrative, there are no provisions that would exempt any of the ''excepted benefits'' from the definition of ''health care.'' It was stated that:

> Although (with the exception of long-term care insurance), the proposed rule does not include the 'excepted benefits' in its list of sixteen examples of a health plan (proposed 45 CFR 160.104), it does not explicitly exclude them either. Because these types of policies in some instances pay benefits that could be construed as payments for medical care, we are concerned by the fact that they are not explicitly excluded from the definition of 'health plan' or the requirements of the proposed rule.''

Several commenters proposed that HHS adopt the same list of ''excepted benefits'' contained in 29 U.S.C. 1191b, suggesting that they could be adopted either as exceptions to the definition of ''health plan'' or as exceptions to the requirements imposed on ''health plans.'' They asserted that this would promote consistency in the federal regulatory structure for health plans.

It was suggested that HHS clarify whether the definition of health plan, particularly the ''group health plan'' and ''health insurance issuer'' components, includes a disability plan or disability insurer. It was noted that a disability plan or disability insurer may cover only income lost from disability and, as mentioned above, some rehabilitation services, or a combination of lost income, rehabilitation services and medical care. The commenter suggested that in addressing this coverage issue, it may be useful to refer to the definitions of group health plan, health insurance issuer and medical care set forth in Part I of HIPAA, which the statutory provisions of the Administrative Simplification subtitle expressly reference. See 42 U.S.C. 1320d(5)(A) and (B).

Response: We agree that the NPRM may have been ambiguous regarding the types of plans the rule covers. To remedy this confusion, we have added language that specifically excludes from the definition any policy, plan, or program providing or paying the cost of the excepted benefits, as defined in section 2971(c)(1) of the PHS Act, 42 U.S.C. 300gg–91(c)(1). As defined in the statute, this includes but is not limited to benefits under one or more (or any combination thereof) of the following: coverage only for accident, or disability income insurance, or any combination thereof; liability insurance, including general liability insurance and automobile liability insurance; and workers' compensation or similar insurance.

However, the other excepted benefits as defined in section 2971(c)(2) of the PHS Act, 42 U.S.C. 300gg–91(c)(2), such as limited scope dental or vision benefits, not explicitly excepted from the regulation could be considered ''health plans'' under paragraph (1)(xvii) of the definition of ''health plan'' in the final rule if and to the extent that they meet the criteria for the definition of ''health plan.'' Such plans, unlike the programs and plans listed at section 2971(c)(1), directly and exclusively provide health insurance, even if limited in scope.

Comment: One commenter recommended that the Secretary clarify that ''health plan'' does not include property and casualty benefit providers. The commenter stated that the clarifying language is needed given the ''catchall'' category of entities defined as ''any other individual plan or group health plan, or combination thereof, that

provides or pays for the cost of medical care,'' and asserted that absent clarification there could be serious confusion as to whether property and casualty benefit providers are ''health plans'' under the rule.

Response: We agree and as described above have added language to the final rule to clarify that the ''excepted benefits'' as defined under 42 U.S.C. 300gg–91(c)(1), which includes liability programs such as property and casualty benefit providers, are not health plans for the purposes of this rule.

Comment: Some commenters recommended that the Secretary replace the term ''medical care'' with ''health care.'' It was observed that ''health care'' was defined in the proposal, and that this definition was used to define what a health care provider does. However, they observed that the definition of ''health plan'' refers to the provision of or payment for ''medical care,'' which is not defined. Another commenter recommended that HHS add the parenthetical phrase ''as such term is defined in section 2791 of the Public Health Service Act'' after the phrase ''medical care.''

Response: We disagree with the first recommendation. We understand that the term ''medical care'' can be easily confused with the term ''health care.'' However, the two terms are not synonymous. The term ''medical care'' is a statutorily defined term and its use is critical in making a determination as to whether a health plan is considered a ''health plan'' for purposes of administrative simplification. In addition, since the term ''medical care'' is used in the regulation only in the context of the definition of ''health plan'' and we believe that its inclusion in the regulatory text may cause confusion, we did not add a definition of ''medical care'' in the final rule. However, consistent with the second recommendation above, the statutory cite for ''medical care'' was added to the definition of ''health plan'' in the Transactions Rule, and thus is reflected in this final rule.

Comment: A number of commenters urged that the Secretary define more narrowly what characteristics would make a government program that pays for specific health care services a ''health plan.'' Commenters argued that there are many ''payment'' programs that should not be included, as discussed below, and that if no distinctions were made, ''health plan'' would mean the same as ''purchaser'' or even ''payor.''

Commenters asserted that there are a number of state programs that pay for ''health care'' (as defined in the rule) but that are not health plans. They said that examples include the WIC program (Special Supplemental Nutrition Program for Women, Infants, and Children) which pays for nutritional assessment and counseling, among other services; the AIDS Client Services Program (including AIDS prescription drug payment) under the federal Ryan White Care Act and state law; the distribution of federal family planning funds under Title X of the Public Health Services Act; and the breast and cervical health program which pays for cancer screening in targeted populations. Commenters argued that these are not insurance plans and do not fall within the ''health plan'' definition's list of examples, all of which are either insurance or broad-scope programs of care under a contract or statutory entitlement. However, paragraph (16) in that list opens the door to broader interpretation through the catchall phrase, ''any other individual or group plan that provides or pays for the cost of medical care.'' Commenters assert that clarification is needed.

A few commenters stated that other state agencies often work in partnership with the state Medicaid program to implement certain Medicaid benefits, such as maternity support services and prenatal genetics screening. They concluded that while this probably makes parts of the agency the ''business partner'' of a covered entity, they were uncertain whether it also makes the same agency parts a ''health plan'' as well.

Response: We agree with the commenters that clarification is needed as to the rule's application to government programs that pay for health care services. Accordingly, in the final rule we have excepted from the definition of ''health plan'' a government funded program which does not have as its principal purpose the provision of, or payment for, the cost of health care or which has as its principal purpose the provision, either directly or by grant, of health care. For example, the principal purpose of the WIC program is not to provide or pay for the cost of health care, and thus, the WIC program is not a health plan for purposes of this rule. The program of health care services for individuals detained by the INS provides health care directly, and so is not a health plan. Similarly, the family planning program authorized by Title X of the Public Health Service Act pays for care exclusively through grants, and so is not a health plan under this rule. These programs (the grantees under the Title X program) may be or include health care providers and may be covered entities if they conduct standard transactions.

We further clarify that, where a public program meets the definition of ''health plan,'' the government agency that administers the program is the covered entity. Where two agencies administer a program jointly, they are both a health plan. For example, both the Health Care Financing Administration and the insurers that offers a Medicare+Choice plan are ''health plans'' with respect to Medicare beneficiaries. An agency that does not administer a program but which provides services for such a program is not a covered entity by virtue of providing such services. Whether an agency providing services is a business associate of the covered entity depends on whether its functions for the covered entity meet the definition of business associate in § 164.501 and, in the example described by this comment, in particular on whether the arrangement falls into the exception in § 164.504(e)(1)(ii)(C) for government agencies that collect eligibility or enrollment information for covered government programs.

Comment: Some commenters expressed support for retaining the category in paragraph (16) of the proposal's definition: ''Any other individual or group health plan, or combination thereof, that provides or pays for the cost of medical care.'' Others asked that the Secretary clarify this category. One commenter urged that the final rule clearly define which plans would meet the criteria for this category.

Response: As described in the proposed rule, this category implements the language at the beginning of the statutory definition of the term ''health plan'': ''The term 'health plan' means an individual or group plan that provides, or pays the cost of, medical care * * * Such term includes the following, and any combination thereof * * *'' This statutory language is general, not specific, and as such, we are leaving it general in the final rule. However, as described above, we add explicit language which excludes certain ''excepted benefits'' from the definition of ''health plan'' in an effort to clarify which plans are not health plans for the purposes of this rule. Therefore, to the extent that a certain benefits plan or program otherwise meets the definition of ''health plan'' and is not explicitly excepted, that program or plan is considered a ''health plan'' under paragraph (1)(xvii) of the final rule.

Comment: A commenter explained that HIPAA defines a group health plan by expressly cross-referencing the statutory sections in the PHS Act and the Employee Retirement Income

Security Act of 1974 (ERISA), 29 U.S.C. 1001, *et seq.*, which define the terms ''group health plan,'' ''employee welfare benefit plan'' and ''participant.'' See 29 U.S.C. 1002(l) (definition of ''employee welfare benefit plan,'' which is the core of the definition of group health plan under both ERISA and the PHS Act); 29 U.S.C. 100217) (definition of participant); 29 U.S.C. 1193(a) (definition of ''group health plan,'' which is identical to that in section 2791(a) of the PHS Act).

It was pointed out that the preamble and the text of the proposed rule both limit the definition of all three terms to their current definitions. The commenter reasoned that since the ERISA definitions may change over time through statutory amendment, Department of Labor regulations or judicial interpretation, it would not be clear what point in time is to be considered current. Therefore, they suggested deleting references to ''current'' or ''currently'' in the preamble and in the regulation with respect to these three ERISA definitions.

In addition, the commenter stated that as the preamble to the NPRM correctly reflected, HIPAA expressly cross-references ERISA's definition of ''participant'' in section 3(7) of ERISA, 29 U.S.C. 1002(7). 42 U.S.C. 1320d(5)(A). The text of the privacy regulation, however, omits this cross-reference. It was suggested that the reference to section 3(7) of ERISA, defining ''participant,'' be included in the regulation.

Finally, HIPAA incorporates the definition of a group health plan as set forth in section 2791(a) of the PHS Act, 42 U.S.C. 300gg–91(a)(l). That definition refers to the provision of medical care ''directly or through insurance, reimbursement, or otherwise.'' The word ''reimbursement'' is omitted in both the preamble and the text of the regulation; the commenter suggested restoring it to both.

Response: We agree. These changes were made to the definition of ''health plan'' as promulgated in the Transactions Rule, and are reflected in this final rule.

Small Health Plan

Comment: One commenter recommended that we delete the reference to $5 million in the definition and instead define a ''small health plan'' as a health plan with fewer than 50 participants. It was stated that using a dollar limitation to define a ''small health plan'' is not meaningful for self-insured plans and some other types of health plan coverage arrangements. A commenter pointed out that the general definition of a health plan refers to ''50 or more participants,'' and that using a dollar factor to define a ''small health plan'' would be inconsistent with this definition.

Response: We disagree. The Small Business Administration (SBA) promulgates size standards that indicate the maximum number of employees or annual receipts allowed for a concern (13 CFR 121.105) and its affiliates to be considered ''small.'' The size standards themselves are expressed either in number of employees or annual receipts (13 CFR 121.201). The size standards for compliance with programs of other agencies are those for SBA programs which are most comparable to the programs of such other agencies, unless otherwise agreed by the agency and the SBA (13 CFR 121.902). With respect to the insurance industry, the SBA has specified that annual receipts of $5 million is the maximum allowed for a concern and its affiliates to be considered small (13 CFR 121.201). Consequently, we retain the proposal's definition in the final rule to be consistent with SBA requirements.

We understand there may be some confusion as to the meaning of ''annual receipts'' when applied to a health plan. For our purposes, therefore, we consider ''pure premiums'' to be equivalent to ''annual receipts.''

Workforce

Comment: Some commenters requested that we exclude ''volunteers'' from the definition of workforce. They stated that volunteers are important contributors within many covered entities, and in particular hospitals. They argued that it was unfair to ask that these people donate their time and at the same time subject them to the penalties placed upon the paid employees by these regulations, and that it would discourage people from volunteering in the health care setting.

Response: We disagree. We believe that differentiating those persons under the direct control of a covered entity who are paid from those who are not is irrelevant for the purposes of protecting the privacy of health information, and for a covered entity's management of its workforce. In either case, the person is working for the covered entity. With regard to implications for the individual, persons in a covered entity's workforce are not held personally liable for violating the standards or requirements of the final rule. Rather, the Secretary has the authority to impose civil monetary penalties and in some cases criminal penalties for such violations on only the covered entity.

Comment: One commenter asked that the rule clarify that employees administering a group health or other employee welfare benefit plan on their employers' behalf are considered part of the covered entity's workforce.

Response: As long as the employees have been identified by the group health plan in plan documents as performing functions related to the group health plan (consistent with the requirements of § 164.504(f)), those employees may have access to protected health information. However, they are not permitted to use or disclose protected health information for employment-related purposes or in connection with any other employee benefit plan or employee benefit of the plan sponsor.

Part 160—Subpart B—Preemption of State Law

We summarize and respond below to comments received in the Transactions rulemaking on the issue of preemption, as well as those received on this topic in the Privacy rulemaking. Because no process was proposed in the Transactions rulemaking for granting exceptions under section 1178(a)(2)(A), a process for making exception determinations was not adopted in the Transactions Rule. Instead, since a process for making exception determinations was proposed in the Privacy rulemaking, we decided that the comments received in the Transactions rulemaking should be considered and addressed in conjunction with the comments received on the process proposed in the Privacy rulemaking. See 65 FR 50318 for a fuller discussion. Accordingly, we discuss the preemption comments received in the Transactions rulemaking where relevant below.

Comment: The majority of comments on preemption addressed the subject in general terms. Numerous comments, particularly from plans and providers, argued that the proposed preemption provisions were burdensome, ineffective, or insufficient, and that complete federal preemption of the ''patchwork'' of state privacy laws is needed. They also argued that the proposed preemption provisions are likely to invite litigation. Various practical arguments in support of this position were made. Some of these comments recognized that the Secretary's authority under section 1178 of the Act is limited and acknowledged that the Secretary's proposals were within her statutory authority. One commenter suggested that the exception determination process would result in a very costly and laborious and sometimes inconsistent analysis of the occasions in which state law would

survive federal preemption, and thus suggested the final privacy regulations preempt state law with only limited exceptions, such as reporting child abuse. Many other comments, however, recommended changing the proposed preemption provisions to preempt state privacy laws on as blanket a basis as possible.

One comment argued that the assumption that more stringent privacy laws are better is not necessarily true, citing a 1999 GAO report finding evidence that the stringent state confidentiality laws of Minnesota halted the collection of comparative information on health care quality.

Several comments in this vein were also received in the Transactions rulemaking. The majority of these comments took the position that exceptions to the federal standards should either be prohibited or discouraged. It was argued that granting exceptions to the standards, particularly the transactions standards, would be inconsistent with the statute's objective of promoting administrative simplification through the use of uniform transactions.

Many other commenters, however, endorsed the ''federal floor'' approach of the proposed rules. (These comments were made in the context of the proposed privacy regulations.) These comments argued that this approach was preferable because it would not impair the effectiveness of state privacy laws that are more protective of privacy, while raising the protection afforded medical information in states that do not enact laws that are as protective as the rules below. Some comments argued, however, that the rules should give even more deference to state law, questioning in particular the definitions and the proposed addition to the ''other purposes'' criterion for exception determinations in this regard.

Response: With respect to the exception process provided for by section 1178(a)(2)(A), the contention that the HIPAA standards should uniformly control is an argument that should be addressed to the Congress, not this agency. Section 1178 of the Act expressly gives the Secretary authority to grant exceptions to the general rule that the HIPAA standards preempt contrary state law in the circumstances she determines come within the provisions at section 1178(a)(2)(A). We agree that the underlying statutory goal of standardizing financial and administrative health care transactions dictates that exceptions should be granted only on narrow grounds. Nonetheless, Congress clearly intended to accommodate some state laws in these areas, and the Department is not free to disregard this Congressional choice. As is more fully explained below, we have interpreted the statutory criteria for exceptions under section 1178(a)(2)(A) to balance the need for relative uniformity with respect to the HIPAA standards with state needs to set certain policies in the statutorily defined areas.

The situation is different with respect to state laws relating to the privacy of protected health information. Many of the comments arguing for uniform standards were particularly concerned with discrepancies between the federal privacy standards and various state privacy requirements. Unlike the situation with respect to the transactions standards, where states have generally not entered the field, all states regulate the privacy of some medical information to a greater or lesser extent. Thus, we understand the private sector's concern at having to reconcile differing state and federal privacy requirements.

This is, however, likewise an area where the policy choice has been made by Congress. Under section 1178(a)(2)(B) of the Act and section 264(c)(2) of HIPAA, provisions of state privacy laws that are contrary to and more stringent than the corresponding federal standard, requirement, or implementation specification are not preempted. The effect of these provisions is to let the law that is most protective of privacy control (the ''federal floor'' approach referred to by many commenters), and this policy choice is one with which we agree. Thus, the statute makes it impossible for the Secretary to accommodate the requests to establish uniformly controlling federal privacy standards, even if doing so were viewed as desirable.

Comment: Numerous comments stated support for the proposal at proposed Subpart B to issue advisory opinions with respect to the preemption of state laws relating to the privacy of individually identifiable health information. A number of these comments appeared to assume that the Secretary's advisory opinions would be dispositive of the issue of whether or not a state law was preempted. Many of these commenters suggested what they saw as improvements to the proposed process, but supported the proposal to have the Department undertake this function.

Response: Despite the general support for the advisory opinion proposal, we decided not to provide specifically for the issuance of such opinions. The following considerations led to this decision. First, the assumption by commenters that an advisory opinion would establish what law applied in a given situation and thereby simplify the task of ascertaining what legal requirements apply to a covered entity or entities is incorrect. Any such opinion would be advisory only. Although an advisory opinion issued by the Department would indicate to covered entities how the Department would resolve the legal conflict in question and would apply the law in determining compliance, it would not bind the courts. While we assume that most courts would give such opinions deference, the outcome could not be guaranteed.

Second, the thousands of questions raised in the public comment about the interpretation, implications, and consequences of all of the proposed regulatory provisions have led us to conclude that significant advice and technical assistance about all of the regulatory requirements will have to be provided on an ongoing basis. We recognize that the preemption concerns that would have been addressed by the proposed advisory opinions were likely to be substantial. However, there is no reason to assume that they will be the most substantial or urgent of the questions that will most likely need to be addressed. It is our intent to provide as much technical advice and assistance to the regulated community as we can with the resources available. Our concern is that setting up an advisory opinion process for just one of the many types of issues that will have to be addressed will lead to a non-optimal allocation of those resources. Upon careful consideration, therefore, we have decided that we will be better able to prioritize our workload and be better able to be responsive to the most urgent and substantial questions raised to the Department, if we do not provide for a formal advisory opinion process on preemption as proposed.

Comment: A few commenters argued that the Privacy Rule should preempt state laws that would impose more stringent privacy requirements for the conduct of clinical trials. One commenter asserted that the existing federal regulations and guidelines for patient informed consent, together with the proposed rule, would adequately protect patient privacy.

Response: The Department does not have the statutory authority under HIPAA to preempt state laws that would impose more stringent privacy requirements on covered entities. HIPAA provides that the rule promulgated by the Secretary may not preempt state laws that are in conflict

with the regulatory requirements and that provide greater privacy protections.

Section 160.201—Applicability

Comment: Several commenters indicated that the guidance provided by the definitions at proposed § 160.202 would be of substantial benefit both to regulated entities and to the public. However, these commenters argued that the applicability of such definitions would be too limited as drafted, since proposed § 160.201 provided that the definitions applied only to ''determinations and advisory opinions issued by the Secretary pursuant to 42 U.S.C. 1320d–7.'' The commenters stated that it would be far more helpful to make the definitions in proposed § 160.202 more broadly applicable, to provide general guidance on the issue of preemption.

Response: We agree with the comments on this issue, and have revised the applicability provision of subpart B below accordingly. Section 160.201 below sets out that Subpart B implements section 1178. This means, in our view, that the definitions of the statutory terms at § 160.202 are legislative rules that apply when those statutory terms are employed, whether by HHS, covered entities, or the courts.

Section 160.202—Definitions

Contrary

Comment: Some commenters asserted that term ''contrary'' as defined at § 160.202 was overly broad and that its application would be time-consuming and confusing for states. These commenters argued that, under the proposed definition, a state would be required to examine all of its laws relating to health information privacy in order to determine whether or not its law were contrary to the requirements proposed. It was also suggested that the definition contain examples of how it would work in practical terms.

A few commenters, however, argued that the definition of ''contrary'' as proposed was too narrow. One commenter argued that the Secretary erred in her assessment of the case law analyzing what is known as ''conflict preemption'' and which is set forth in shorthand in the tests set out at § 160.202.

Response: We believe that the definition proposed represents a policy that is as clear as is feasible and which can be applied nationally and uniformly. As was noted in the preamble to the proposed rules (at 64 FR 59997), the tests in the proposed definition of ''contrary'' are adopted from the jurisprudence of ''conflict preemption.'' Since preemption is a judicially developed doctrine, it is reasonable to interpret this term as indicating that the statutory analysis should tie in to the analytical formulations employed by the courts. Also, while the court-developed tests may not be as clear as commenters would like, they represent a long-term, thoughtful consideration of the problem of defining when a state/federal conflict exists. They will also, we assume, generally be employed by the courts when conflict issues arise under the rules below. We thus see no practical alternative to the proposed definition and have retained it unchanged. With respect to various suggestions for shorthand versions of the proposed tests, such as the arguably broader term ''inconsistent with,'' we see no operational advantages to such terms.

Comment: One comment asked that the Department clarify that if state law is not preempted, then the federal law would not also apply.

Response: This comment raises two issues, both of which deserve discussion. First, a state law may not be preempted because there is no conflict with the analogous federal requirement; in such a situation, both laws can, and must, be complied with. We thus do not accept this suggestion, to the extent that it suggests that the federal law would give way in this situation. Second, a state law may also not be preempted because it comes within section 1178(a)(2)(B), section 1178(b), or section 1178(c); in this situation, a contrary federal law would give way.

Comment: One comment urged the Department to take the position that where state law exists and no analogous federal requirement exists, the state requirement would not be ''contrary to'' the federal requirement and would therefore not trigger preemption.

Response: We agree with this comment.

Comment: One commenter criticized the definition as unhelpful in the multi-state transaction context. For example, it was asked whether the issue of whether a state law was ''contrary to'' should be determined by the law of the state where the treatment is provided, where the claim processor is located, where the payment is issued, or the data maintained, assuming all are in different states.

Response: This is a choice of law issue, and, as is discussed more fully below, is a determination that is routinely made today in connection with multi-state transactions. See discussion below under Exception Determinations (Criteria for Exception Determinations).

State Law

Comment: Comments noted that the definition of ''state law'' does not explicitly include common law and recommended that it be revised to do so or to clarify that the term includes evidentiary privileges recognized at state law. Guidance concerning the impact of state privileges was also requested.

Response: As requested, we clarify that the definition of ''state law'' includes common law by including the term ''common law.'' In our view, this phrase encompasses evidentiary privileges recognized at state law (which may also, we note, be embodied in state statutes).

Comment: One comment criticized this definition as unwieldy, in that locating state laws pertaining to privacy is likely to be difficult. It was noted that Florida, for example, has more than 60 statutes that address health privacy.

Response: To the extent that state laws currently apply to covered entities, they have presumably determined what those laws require in order to comply with them. Thus, while determining which laws are ''contrary'' to the federal requirements will require additional work in terms of comparing state law with the federal requirements, entities should already have acquired the knowledge of state law needed for this task in the ordinary course of doing business.

Comment: The New York City Department of Health noted that in many cases, provisions of New York State law are inapplicable within New York City, because the state legislature has recognized that the local code is tailored to the particular needs of the City. It urged that the New York City Code be treated as state law, for preemption purposes.

Response: We agree that, to the extent a state treats local law as substituting for state law it could be considered to be ''state law'' for purposes of this definition. If, however, a local law is local in scope and effect, and a tier of state law exists over the same subject matter, we do not think that the local law could or should be treated as ''state law'' for preemption purposes. We do not have sufficient information to assess the situation raised by this comment with respect to this principle, and so express no opinion thereon.

More Stringent

Comment: Many commenters supported the policy in the proposed definition of ''individual'' at proposed § 164.502, which would have permitted unemancipated minors to exercise, on

their own behalf, rights granted to individuals in cases where they consented to the underlying health care. Commenters stated, however, that the proposed preemption provision would leave in place state laws authorizing or prohibiting disclosure to parents of the protected health information of their minor children and would negate the proposed policy for the treatment of minors under the rule. The comments stated that such state laws should be treated like other state laws, and preempted to the extent that they are less protective of the privacy of minors.

Other commenters supported the proposed preemption provision—not to preempt a state law to the extent it authorizes or prohibits disclosure of protected health information regarding a minor to a parent.

Response: Laws regarding access to health care for minors and confidentiality of their medical records vary widely; this regulation recognizes and respects the current diversity of state law in this area. Where states have considered the balance involved in protecting the confidentiality of minors' health information and have explicitly acted, for example, to authorize disclosure, defer the decision to disclose to the discretion of the health care provider, or prohibit disclosure of minor's protected health information to a parent, the rule defers to these decisions to the extent that they regulate such disclosures.

Comment: The proposed definition of ''more stringent'' was criticized as affording too much latitude to for granting exceptions for state laws that are not protective of privacy. It was suggested that the test should be ''most protective of the individual's privacy.''

Response: We considered adopting this test. However, for the reasons set out at 64 FR 59997, we concluded that this test would not provide sufficient guidance. The comments did not address the concerns we raised in this regard in the preamble to the proposed rules, and we continue to believe that they are valid.

Comment: A drug company expressed concern with what it saw as the expansive definition of this term, arguing that state governments may have less experience with the special needs of researchers than federal agencies and may unknowingly adopt laws that have a deleterious effect on research. A provider group expressed concern that allowing stronger state laws to prevail could result in diminished ability to get enough patients to complete high quality clinical trials.

Response: These concerns are fundamentally addressed to the ''federal floor'' approach of the statute, not to the definition proposed: even if the definition of ''more stringent'' were narrowed, these concerns would still exist. As discussed above, since the ''federal floor'' approach is statutory, it is not within the Secretary's authority to change the dynamics that are of concern.

Comment: One comment stated that the proposed rule seemed to indicate that the ''more stringent'' and ''contrary to'' definitions implied that these standards would apply to ERISA plans as well as to non-ERISA plans.

Response: The concern underlying this comment is that ERISA plans, which are not now subject to certain state laws because of the ''field'' preemption provision of ERISA but which are subject to the rules below, will become subject to state privacy laws that are ''more stringent'' than the federal requirements, due to the operation of section 1178(a)(2)(B), together with section 264(c)(2). We disagree that this is the case. While the courts will have the final say on these questions, it is our view that these sections simply leave in place more stringent state laws that would otherwise apply; to the extent that such state laws do not apply to ERISA plans because they are preempted by ERISA, we do not think that section 264(c)(2) overcomes the preemption effected by section 514(a) of ERISA. For more discussion of this point, see 64 FR 60001.

Comment: The Lieutenant Governor's Office of the State of Hawaii requested a blanket exemption for Hawaii from the federal rules, on the ground that its recently enacted comprehensive health privacy law is, as a whole, more stringent than the proposed federal standards. It was suggested that, for example, special weight should be given to the severity of Hawaii's penalties. It was suggested that a new definition (''comprehensive'') be added, and that ''more stringent'' be defined in that context as whether the state act or code as a whole provides greater protection.

An advocacy group in Vermont argued that the Vermont legislature was poised to enact stronger and more comprehensive privacy laws and stated that the group would resent a federal prohibition on that.

Response: The premise of these comments appears to be that the provision-by-provision approach of Subpart B, which is expressed in the definition of the term ''contrary'', is wrong. As we explained in the preamble to the proposed rules (at 64 FR 59995), however, the statute dictates a provision-by-provision comparison of state and federal requirements, not the overall comparison suggested by these comments. We also note that the approach suggested would be practically and analytically problematic, in that it would be extremely difficult, if not impossible, to determine what is a legitimate stopping point for the provisions to be weighed on either the state side or the federal side of the scale in determining which set of laws was the ''more stringent.'' We accordingly do not accept the approach suggested by these comments.

With respect to the comment of the Vermont group, nothing in the rules below prohibits or places any limits on states enacting stronger or more comprehensive privacy laws. To the extent that states enact privacy laws that are stronger or more comprehensive than contrary federal requirements, they will presumably not be preempted under section 1178(a)(2)(B). To the extent that such state laws are not contrary to the federal requirements, they will act as an overlay on the federal requirements and will have effect.

Comment: One comment raised the issue of whether a private right of action is a greater penalty, since the proposed federal rule has no comparable remedy.

Response: We have reconsidered the proposed ''penalty'' provision of the proposed definition of ''more stringent'' and have eliminated it. The HIPAA statute provides for only two types of penalties: fines and imprisonment. Both types of penalties could be imposed in addition to the same type of penalty imposed by a state law, and should not interfere with the imposition of other types of penalties that may be available under state law. Thus, we think it is unlikely that there would be a conflict between state and federal law in this respect, so that the proposed criterion is unnecessary and confusing. In addition, the fact that a state law allows an individual to file a lawsuit to protect privacy does not conflict with the HIPAA penalty provisions.

Relates to the Privacy of Individually Identifiable Health Information

Comment: One comment criticized the definition of this term as too narrow in scope and too uncertain. The commenter argued that determining the specific purpose of a state law may be difficult and speculative, because many state laws have incomplete, inaccessible, or non-existent legislative histories. It was suggested that the definition be revised by deleting the word ''specific'' before the word ''purpose.'' Another commenter argued

that the definition of this term should be narrowed to minimize reverse preemption by more stringent state laws. One commenter generally supported the proposed definition of this term.

Response: We are not accepting the first comment. The purpose of a given state enactment should be ascertainable, if not from legislative history or a purpose statement, then from the statute viewed as a whole. The same should be true of state regulations or rulings. In any event, it seems appropriate to restrict the field of state laws that may potentially trump the federal standards to those that are clearly intended to establish state public policy and operate in the same area as the federal standards. To the extent that the definition in the rules below does this, we have accommodated the second comment. We note, however, that we do not agree that the definition should be further restricted to minimize ''reverse preemption,'' as suggested by this comment, as we believe that state laws that are more protective of privacy than contrary federal standards should remain, in order to ensure that the privacy of individuals' health information receives the maximum legal protection available.

Sections 160.203 and 160.204—Exception Determinations and Advisory Opinions

Most of the comments received on proposed Subpart B lumped together the proposed process for exception determinations under section 1178(a)(2)(A) with the proposed process for issuing advisory opinions under section 1178(a)(2)(B), either because the substance of the comment applied to both processes or because the commenters did not draw a distinction between the two processes. We address these general comments in this section.

Comment: Numerous commenters, particularly providers and provider groups, recommended that exception determinations and advisory opinions not be limited to states and advocated allowing all covered entities (including individuals, providers and insurers), or private sector organizations, to request determinations and opinions with respect to preemption of state laws. Several commenters argued that limiting requests to states would deny third party stakeholders, such as life and disability income insurers, any means of resolving complex questions as to what rule they are subject to. One commenter noted that because it is an insurer who will be liable if it incorrectly analyzes the interplay between laws and reaches an incorrect conclusion, there would be little incentive for the states to request clarification. It would also cause large administrative burdens which, it was stated, would be costly and confusing. It was also suggested that the request for the exception be made to the applicable state's attorney general or chief legal officer, as well as the Secretary. Various changes to the language were suggested, such as adding that ''a covered entity, or any other entity impacted by this rule'' be allowed to submit the written request.

Response: We agree, and have changed § 164.204(a) below accordingly.

The decision to eliminate advisory opinions makes this issue moot with respect to those opinions.

Comment: Several commenters noted that it was unclear under the proposed rule which state officials would be authorized to request a determination.

Response: We agree that the proposed rule was unclear in this respect. The final rule clarifies who may make the request for a state, with respect to exception determinations. See, § 160.204(a). The language adopted should ensure that the Secretary receives an authoritative statement from the state. At the same time, this language provides states with flexibility, in that the governor or other chief elected official may choose to designate other state officials to make such requests.

Comment: Many commenters recommended that a process be established whereby HHS performs an initial state-by-state critical analysis to provide guidance on which state laws will not be preempted; most suggested that such an analysis (alternatively referred to as a database or clearinghouse) should be completed before providers would be required to come into compliance. Many of these comments argued that the Secretary should bear the cost for the analyses of state law, disagreeing with the premise stated in the preamble to the proposed rules that it is more efficient for the private market to complete the state-by-state review. Several comments also requested that HHS continue to maintain and monitor the exception determination process, and update the database over time in order to provide guidance and certainty on the interaction of the federal rules with newly enacted or amended state laws that are produced after the final rule. Some comments recommended that each state be required to certify agreement with the HHS analyses.

In contrast, one hospital association noted concerns that the Secretary would conduct a nationwide analysis of state laws. The comment stated that implementation would be difficult since much of the law is a product of common law, and such state-specific research should only be attempted by experienced health care attorneys in each jurisdiction.

Response: These comments seem to be principally concerned with potential conflicts between state privacy laws and the privacy standards, because, as is more fully explained below, preemption of contrary state laws not relating to privacy is automatic unless the Secretary affirmatively acts under section 1178(a)(2)(A) to grant an exception. We recognize that the provisions of sections 1178(b) (state public health laws), and 1178(c) (state regulation of health plans) similarly preserve state laws in those areas, but very little of the public comment appeared to be concerned with these latter statutory provisions. Accordingly, we respond below to what we see as the commenters' main concern.

The Department will not do the kind of global analysis requested by many of these comments. What these comments are in effect seeking is a global advisory opinion as to when the federal privacy standards will control and when they will not. We understand the desire for certainty underlying these comments. Nonetheless, the reasons set out above as the basis for our decision not to establish a formal advisory opinion process apply equally to these requests. We also do not agree that the task of evaluating the requirements below in light of existing state law is unduly burdensome or unreasonable. Rather, it is common for new federal requirements to necessitate an examination by the regulated entities of the interaction between existing state law and the federal requirements incident to coming into compliance.

We agree, however, that the case is different where the Secretary has affirmatively acted, either through granting an exception under section 1178(a)(2)(A) or by making a specific determination about the effect of a particular state privacy law in, for example, the course of determining an entity's compliance with the privacy standards. As is discussed below, the Department intends to make notice of exception determinations that it makes routinely available.

We do not agree with the comments suggesting that compliance by covered entities be delayed pending completion of an analysis by the Secretary and that states be required to certify agreement with the Secretary's analysis, as we are not institutionalizing the advisory opinion/analysis process upon which these comments are predicated.

Furthermore, with respect to the suggestion regarding delaying the compliance date, Congress provided in section 1175(b) of the Act for a delay in when compliance is required to accommodate the needs of covered entities to address implementation issues such as those raised by these comments. With respect to the suggestion regarding requiring states to certify their agreement with the Secretary's analysis, we have no authority to do this.

Comment: Several commenters criticized the proposed provision for annual publication of determinations and advisory opinions in the **Federal Register** as inadequate. They suggested that more frequent notices should be made and the regulation be changed accordingly, to provide for publication either quarterly or within a few days of a determination. A few commenters suggested that any determinations made, or opinions issued, by the Secretary be published on the Department's website within 10 days or a few days of the determination or opinion.

Response: We agree that the proposed provision for annual publication was inadequate and have accordingly deleted it. Subpart B contains no express requirement for publication, as the Department is free to publish its determinations absent such a requirement. It is our intention to publish notice of exception determinations on a periodic basis in the **Federal Register**. We will also consider other avenues of making such decisions publicly available as we move into the implementation process.

Comment: A few commenters argued that the process for obtaining an exception determination or an advisory opinion from the Secretary will result in a period of time in which there is confusion as to whether state or federal law applies. The proposed regulations say that the federal provisions will remain effective until the Secretary makes a determination concerning the preemption issue. This means that, for example, a state law that was enacted and enforced for many years will be preempted by federal law for the period of time during which it takes the Secretary to make a determination. Then if the Secretary determines that the state law is not preempted, the state law will again become effective. Such situations will result in confusion and unintended violations of the law. One of the commenters suggested that requests for exceptions be required only when a challenge is brought against a particular state law, and that a presumption of validity should lie with state laws. Another commenter, however, urged that ''instead of the presumption of preemption, the state laws in question would be presumed to be subject to the exception unless or until the Secretary makes a determination to the contrary.''

Response: It is true that the effect of section 1178(a)(2)(A) is that the federal standards will preempt contrary state law and that such preemption will not be removed unless and until the Secretary acts to grant an exception under that section (assuming, of course, that another provision of section 1178 does not apply). We do not agree, however, that confusion should result, where the issue is whether a given state law has been preempted under section 1178(a)(2)(A). Because preemption is automatic with respect to state laws that do not come within the other provisions of section 1178 (i.e., sections 1178(a)(2)(B), 1178(b), and 1178(c)), such state laws are preempted until the Secretary affirmatively acts to preserve them from preemption by granting an exception under section 1178(a)(2)(A).

We cannot accept the suggestion that a presumption of validity attach to state laws, and that states not be required to request exceptions except in very narrow circumstances. The statutory scheme is the opposite: The statute effects preemption in the section 1178(a)(2)(A) context unless the Secretary affirmatively acts to except the contrary state law in question.

With respect to preemption under sections 1178(b) and 1178(c) (the carve-outs for state public health laws and state regulation of health plans), we do not agree that preemption is likely to be a major cause of uncertainty. We have deferred to Congressional intent by crafting the permissible releases for public health, abuse, and oversight broadly. See, §§ 164.512(b)—(d) below. Since there must first be a conflict between a state law and a federal requirement in order for an issue of preemption to even arise, we think that, as a practical matter, few preemption questions should arise with respect to sections 1178(b) and 1178(c).

With respect to preemption of state privacy laws under section 1178(a)(2)(B), however, we agree that the situation may be more difficult to ascertain, because the Secretary does not determine the preemption status of a state law under that section, unlike the situation with respect to section 1178(a)(2)(A). We have tried to define the term ''more stringent'' to identify and particularize the factors to be considered by courts to those relevant to privacy interests. The more specific (than the statute) definition of this term at § 160.202 below should provide some guidance in making the determination as to which law prevails. Ambiguity in the state of the law might also be a factor to be taken into account in determining whether a penalty should be applied.

Comment: Several comments recommended that exception determinations or advisory opinions encompass a state act or code in its entirety (in lieu of a provision-specific evaluation) if it is considered more stringent as a whole than the regulation. It was argued that since the provisions of a given law are typically interconnected and related, adopting or overriding them on a provision-by-provision basis would result in distortions and/or unintended consequences or loopholes. For example, when a state law includes authorization provisions, some of which are consistent with the federal requirements and some which are not, the cleanest approach is to view the state law as inconsistent with the federal requirements and thus preempted in its entirety. Similarly, another comment suggested that state confidentiality laws written to address the specific needs of individuals served within a discreet system of care be considered as a whole in assessing whether they are as stringent or more stringent than the federal requirements. Another comment requested explicit clarification that state laws with a broader scope than the regulation will be viewed as more stringent and be allowed to stand.

Response: We have not adopted the approach suggested by these comments. As discussed above with respect to the definition of the term ''more stringent,'' it is our view that the statute precludes the approach suggested. We also suggest that this approach ignores the fact that each separate provision of law usually represents a nuanced policy choice to, for example, permit this use or prohibit that disclosure; the aggregated approach proposed would fail to recognize and weigh such policy choices.

Comment: One comment recommended that the final rule: permit requests for exception determinations and advisory opinions as of the date of publication of the final rule, require the Secretary to notify the requestor within a specified short period of time of all additional information needed, and prohibit enforcement action until the Secretary issues a response.

Response: With respect to the first recommendation, we clarify that requests for exception determinations may be made at any time; since the process for issuing advisory opinions has not been adopted, this recommendation is moot as it pertains

to advisory opinions. With respect to the second recommendation, we will undertake to process exception requests as expeditiously as possible, but, for the reasons discussed below in connection with the comments relating to setting deadlines for those determinations, we cannot commit at this time to a ''specified short period of time'' within which the Secretary may request additional information. We see no reason to agree to the third recommendation. Because contrary state laws for which an exception is available only under section 1178(a)(2)(A) will be preempted by operation of law unless and until the Secretary acts to grant an exception, there will be an ascertainable compliance standard for compliance purposes, and enforcement action would be appropriate where such compliance did not occur.

Sections 160.203(a) and 160.204(a)—Exception Determinations

Section 160.203(a)—Criteria for Exception Determinations

Comment: Numerous comments criticized the proposed criteria for their substance or lack thereof. A number of commenters argued that the effectiveness language that was added to the third statutory criterion made the exception so massive that it would swallow the rule. These comments generally expressed concern that laws that were less protective of privacy would be granted exceptions under this language. Other commenters criticized the criteria generally as creating a large loophole that would let state laws that do not protect privacy trump the federal privacy standards.

Response: We agree with these comments. The scope of the statutory criteria is ambiguous, but they could be read so broadly as to largely swallow the federal protections. We do not think that this was Congress's intent. Accordingly, we have added language to most of the statutory criteria clarifying their scope. With respect to the criteria at 1178(a)(2)(A)(i), this clarifying language generally ties the criteria more specifically to the concern with protecting and making more efficient the health care delivery and payment system that underlies the Administrative Simplification provisions of HIPAA, but, with respect to the catch-all provision at section 1178(a)(2)(A)(i)(IV), also requires that privacy interests be balanced with such concerns, to the extent relevant. We require that exceptions for rules to ensure appropriate state regulation of insurance and health plans be stated in a statute or regulation, so that such exceptions will be clearly tied to statements of priorities made by publicly accountable bodies (e.g., through the public comment process for regulations, and by elected officials through statutes). With respect to the criterion at section 1178(a)(2)(A)(ii), we have further delineated what ''addresses controlled substances'' means. The language provided, which builds on concepts at 21 U.S.C. 821 and the Medicare regulations at 42 CFR 1001.2, delineates the area within which the government traditionally regulates controlled substances, both civilly and criminally; it is our view that HIPAA was not intended to displace such regulation.

Comment: Several commenters urged that the request for determination by the Secretary under proposed § 160.204(a) be limited to cases where an exception is absolutely necessary, and that in making such a determination, the Secretary should be required to make a determination that the benefits of granting an exception outweigh the potential harm and risk of disclosure in violation of the regulation.

Response: We have not further defined the statutory term ''necessary'', as requested. We believe that the determination of what is ''necessary'' will be fact-specific and context dependent, and should not be further circumscribed absent such specifics. The state will need to make its case that the state law in question is sufficiently ''necessary'' to accomplish the particular statutory ground for exception that it should trump the contrary federal standard, requirement, or implementation specification.

Comment: One commenter noted that a state should be required to explain whether it has taken any action to correct any less stringent state law for which an exception has been requested. This commenter recommended that a section be added to proposed § 160.204(a) stating that ''a state must specify what, if any, action has been taken to amend the state law to comply with the federal regulations.'' Another comment, received in the Transactions rulemaking, took the position that exception determinations should be granted only if the state standards in question exceeded the national standards.

Response: The first and last comments appear to confuse the ''more stringent'' criterion that applies under section 1178(a)(2)(B) of the Act with the criteria that apply to exceptions under section 1178(a)(2)(A). We are also not adopting the language suggested by the first comment, because we do not agree that states should necessarily have to try to amend their state laws as a precondition to requesting exceptions under section 1178(a)(2)(A). Rather, the question should be whether the state has made a convincing case that the state law in question is sufficiently necessary for one of the statutory purposes that it should trump the contrary federal policy.

Comment: One commenter stated that exceptions for state laws that are contrary to the federal standards should not be preempted where the state and federal standards are found to be equal.

Response: This suggestion has not been adopted, as it is not consistent with the statute. With respect to the administrative simplification standards in general, it is clear that the intent of Congress was to preempt contrary state laws except in the limited areas specified as exceptions or carve-outs. See, section 1178. This statutory approach is consistent with the underlying goal of simplifying health care transactions through the adoption of uniform national standards. Even with respect to state laws relating to the privacy of medical information, the statute shields such state laws from preemption by the federal standards only if they are ''more'' stringent than the related federal standard or implementation specification.

Comment: One commenter noted that determinations would apply only to transactions that are wholly intrastate. Thus, any element of a health care transaction that would implicate more than one state's law would automatically preclude the Secretary's evaluation as to whether the laws were more or less stringent than the federal requirement. Other commenters expressed confusion about this proposed requirement, noting that providers and plans operate now in a multi-state environment.

Response: We agree with the commenters and have dropped the proposed requirement. As noted by the commenters, health care entities now typically operate in a multi-state environment, so already make the choice of law judgements that are necessary in multi-state transactions. It is the result of that calculus that will have to be weighed against the federal standards, requirements, and implementation specifications in the preemption analysis.

Comment: One comment received in the Transactions rulemaking suggested that the Department should allow exceptions to the standard transactions to accommodate abbreviated transactions between state agencies, such as claims between a public health department and the state Medicaid

agency. Another comment requested an exception for Home and Community Based Waiver Services from the transactions standards.

Response: The concerns raised by these comments would seem to be more properly addressed through the process established for maintaining and modifying the transactions standards. If the concerns underlying these comments cannot be addressed in this manner, however, there is nothing in the rules below to preclude states from requesting exceptions in such cases. They will then have to make the case that one or more grounds for exception applies.

Section 160.204(a)—Process for Exception Determinations—Comments and Responses

Comment: Several comments received in the Transactions rulemaking stated that the process for applying for and granting exception determinations (referred to as ''waivers'' by some) needed to be spelled out in the final rule.

Response: We agree with these comments. As noted above, since no process was proposed in the Transactions rulemaking, a process for making exception determinations was not adopted in those final rules. Subpart B below adopts a process for making exception determinations, which responds to these comments.

Comment: Comments stated that the exception process would be burdensome, unwieldy, and time-consuming for state agencies as well as the Department. One comment took the position that states should not be required to submit exception requests to the Department under proposed § 160.203(a), but could provide documentation that the state law meets one of the conditions articulated in proposed § 160.203.

Response: We disagree that the process adopted at § 164.204 below will be burdensome, unwieldy, or time-consuming. The only thing the regulation describes is the showings that a requestor must make as part of its submission, and all are relevant to the issue to be determined by the Secretary. How much information is submitted is, generally speaking, in the requestor's control, and the regulation places no restrictions on how the requestor obtains it, whether by acting directly, by working with providers and/or plans, or by working with others. With respect to the suggestion that states not be required to submit exception requests, we disagree that this suggestion is either statutorily authorized or advisable. We read this comment as implicitly suggesting that the Secretary must proactively identify instances of conflict and evaluate them. This suggestion is, thus, at bottom the same as the many suggestions that we create a database or compendium of controlling law, and it is rejected for the same reasons.

Comment: Several comments urged that all state requests for non-preemption include a process for public participation. These comments believe that members of the public and other interested stakeholders should be allowed to submit comments on a state's request for exception, and that these comments should be reviewed and considered by the Secretary in determining whether the exception should be granted. One comment suggested that the Secretary at least give notice to the citizens of the state prior to granting an exception.

Response: The revision to § 160.204(a), to permit requests for exception determinations by any person, responds to these comments.

Comment: Many commenters noted that the lack of a clear and reasonable time line for the Secretary to issue an exception determination would not provide sufficient assurance that the questions regarding what rules apply will be resolved in a time frame that will allow business to be conducted properly, and argued that this would increase confusion and uncertainty about which statutes and regulations should be followed. Timeframes of 60 or 90 days were suggested. One group suggested that, if a state does not receive a response from HHS within 60 days, the waiver should be deemed approved.

Response: The workload prioritization and management considerations discussed above with respect to advisory opinions are also relevant here and make us reluctant to agree to a deadline for making exception determinations. This is particularly true at the outset, since we have no experience with such requests. We therefore have no basis for determining how long processing such requests will take, how many requests we will need to process, or what resources will be available for such processing. We agree that states and other requesters should receive timely responses and will make every effort to make determinations as expeditiously as possible, but we cannot commit to firm deadlines in this initial rule. Once we have experience in handling exception requests, we will consult with states and others in regard to their experiences and concerns and their suggestions for improving the Secretary's expeditious handling of such requests.

We are not accepting the suggestion that requests for exception be deemed approved if not acted upon in some defined time period. Section 1178(a)(2)(A) requires a specific determination by the Secretary. The suggested policy would not be consistent with this statutory requirement. It is also inadvisable from a policy standpoint, in that it would tend to maximize exceptions. This would be contrary to the underlying statutory policy in favor of uniform federal standards.

Comment: One commenter took exception to the requirement for states to seek a determination from the Department that a provision of state law is necessary to prevent fraud and abuse or to ensure appropriate state regulation of insurance plans, contending that this mandate could interfere with the Insurance Commissioners' ability to do their jobs. Another commenter suggested that the regulation specifically recognize the broad scope of state insurance department activities, such as market conduct examinations, enforcement investigations, and consumer complaint handling.

Response: The first comment raises an issue that lies outside our legal authority to address, as section 1178(a)(2)(A) clearly mandates that the Secretary make a determination in these areas. With respect to the second comment, to the extent these concerns pertain to health plans, we believe that the provisions at § 164.512 relating to oversight and disclosures required by law should address the concerns underlying this comment.

Section 160.204(a)(4)—Period of Effectiveness of Exception Determinations

Comment: Numerous commenters stated that the proposed three year limitation on the effectiveness of exception determinations would pose significant problems and should be limited to one year, since a one year limitation would provide more frequent review of the necessity for exceptions. The commenters expressed concern that state laws which provide less privacy protection than the federal regulation would be given exceptions by the Secretary and thus argued that the exceptions should be more limited in duration or that the Secretary should require that each request, regardless of duration, include a description of the length of time such an exception would be needed.

One state government commenter, however, argued that the 3 year limit should be eliminated entirely, on the ground that requiring a redetermination

every three years would be burdensome for the states and be a waste of time and resources for all parties. Other commenters, including two state agencies, suggested that the exemption should remain effective until either the state law or the federal regulation is changed. Another commenter suggested that the three year sunset be deleted and that the final rule provide for automatic review to determine if changes in circumstance or law would necessitate amendment or deletion of the opinion. Other recommendations included deeming the state law as continuing in effect upon the submission of a state application for an exemption rather than waiting for a determination by the Secretary that may not occur for a substantial period of time.

Response: We are persuaded that the proposed 3 year limit on exception determinations does not make sense where neither law providing the basis for the exception has changed in the interim. We also agree that where either law has changed, a previously granted exception should not continue. Section 160.205(a) below addresses these concerns.

Sections 160.203(b) and 160.204(b)—Advisory Opinions

Section 160.203(b)—Effect of Advisory Opinions

Comment: Several commenters questioned whether or not DHHS has standing to issue binding advisory opinions and recommended that the Department clarify this issue before implementation of this regulation. One respondent suggested that the Department clarify in the final rule the legal issues on which it will opine in advisory opinion requests, and state that in responding to requests for advisory opinions the Department will not opine on the preemptive force of ERISA with respect to state laws governing the privacy of individually identifiable health information, since interpretations as to the scope and extent of ERISA's preemption provisions are outside of the Department's jurisdictional authority.

One commenter asked whether a state could enforce a state law which the Secretary had indicated through an advisory opinion is preempted by federal law. This commenter also asked whether the state would be subject to penalties if it chose to continue to enforce its own laws.

Response: As discussed above, in part for reasons raised by these comments, the Department has decided not to have a formal process for issuing advisory opinions, as proposed.

Several of these concerns, however, raise issues of broader concern that need to be addressed. First, we disagree that the Secretary lacks legal authority to opine on whether or not state privacy laws are preempted. The Secretary is charged by law with determining compliance, and where state law and the federal requirements conflict, a determination of which law controls will have to be made in order to determine whether the federal standard, requirement, or implementation specification at issue has been violated. Thus, the Secretary cannot carry out her enforcement functions without making such determinations. It is further reasonable that, if the Secretary makes such determinations, she can make those determinations known, for whatever persuasive effect they may have.

The questions as to whether a state could enforce, or would be subject to penalties if it chose to continue to enforce, its own laws following a denial by the Secretary of an exception request under § 160.203 or a holding by a court of competent jurisdiction that a state privacy law had been preempted by a contrary federal privacy standard raise several issues. First, a state law is preempted under the Act only to the extent that it applies to covered entities; thus, a state is free to continue to enforce a ''preempted'' state law against non-covered entities to which the state law applies. If there is a question of coverage, states may wish to establish processes to ascertain which entities within their borders are covered entities within the meaning of these rules. Second, with respect to covered entities, if a state were to try to enforce a preempted state law against such entities, it would presumably be acting without legal authority in so doing. We cannot speak to what remedies might be available to covered entities to protect themselves against such wrongful state action, but we assume that covered entities could seek judicial relief, if all else failed. With respect to the issue of imposing penalties on states, we do not see this as likely. The only situation that we can envision in which penalties might be imposed on a state would be if a state agency were itself a covered entity and followed a preempted state law, thereby violating the contrary federal standard, requirement, or implementation specification.

Section 160.204(b)—Process for Advisory Opinions

Comment: Several commenters stated that it was unclear whether a state would be required to submit a request for an advisory opinion in order for the law to be considered more stringent and thus not preempted. The Department should clarify whether a state law could be non-preempted even without such an advisory opinion. Another commenter requested that the final rule explicitly state that the stricter rule always applies, whether it be state or federal, and regardless of whether there is any conflict between state and federal law.

Response: The elimination of the proposed process for advisory opinions renders moot the first question. Also, the preceding response clarifies that which law preempts in the privacy context (assuming that the state law and federal requirement are ''contrary'') is a matter of which one is the ''more stringent.'' This is not a matter which the Secretary will ultimately determine; rather, this is a question about which the courts will ultimately make the final determination. With respect to the second comment, we believe that § 160.203(b) below responds to this issue, but we would note that the statute already provides for this.

Comment: Several commenters supported the decision to limit the parties who may request advisory opinions to the state. These commenters did not believe that insurers should be allowed to request an advisory opinion and open every state law up to challenge and review.

Several commenters requested that guidance on advisory opinions be provided in *all* circumstances, not only at the Secretary's discretion. It was suggested that proposed § 160.204(b)(2)(iv) be revised to read as follows: ''A state may submit a written request to the Secretary for an advisory opinion under this paragraph. The request must include the following information: the reasons why the state law *should* or *should not be* preempted by the federal standard, requirement, or implementation specification, including how the state law meets the criteria at § 160.203(b).''

Response: The decision not to have a formal process for issuing advisory opinions renders these issues moot.

Sections 160.203(c) and 160.203(d)—Statutory Carve-Outs

Comment: Several commenters asked that the Department provide more specific examples itemizing activities traditionally regulated by the state that could constitute ''carve-out'' exceptions. These commenters also requested that the Department include language in the regulation stating that if a state law falls within several different exceptions, the state chooses which determination exception shall apply.

Response: We are concerned that itemizing examples in this way could leave out important state laws or create inadvertent negative implications that laws not listed are not included. However, as explained above, we have designed the types of activities that are permissive disclosures for public health under § 164.512(b) below in part to come within the carve-out effected by section 1178(b); while the state regulatory activities covered by section 1178(c) will generally come within § 164.512(d) below. With respect to the comments asking that a state get to ''choose'' which exception it comes under, we have in effect provided for this with respect to exceptions under section 1178(a)(2)(A), by giving the state the right to request an exception under that section. With respect to exceptions under section 1178(a)(2)(B), those exceptions occur by operation of law, and it is not within the Secretary's power to ''let'' the state choose whether an exception occurs under that section.

Comment: Several commenters took the position that the Secretary should not limit the procedural requirements in proposed § 160.204(a) to only those applications under proposed § 160.203(a). They urged that the requirements of proposed § 160.204(a) should also apply to preemption under sections 1178(a)(2)(B), 1178(b) and 1178(c). It was suggested that the rules should provide for exception determinations with respect to the matters covered by these provisions of the statute; such additional provisions would provide clear procedures for states to follow and ensure that requests for exceptions are adequately documented.

A slightly different approach was taken by several commenters, who recommended that proposed § 160.204(b) be amended to clarify that the Secretary will also issue advisory opinions as to whether a state law constitutes an exception under proposed §§ 160.203(c) and 160.203(d). This change would, they argued, give states the same opportunity for guidance that they have under § 160.203(a) and (b), and as such, avoid costly lawsuits to preserve state laws.

Response: We are not taking either of the recommended courses of action. With respect to the recommendation that we expand the exception determination process to encompass exceptions under sections 1178(a)(2)(B), 1178(b), and 1178(c), we do not have the authority to grant exceptions under these sections. Under section 1178, the Secretary has authority to make exception determinations only with respect to the matters covered by section 1178(a)(2)(A); contrary state laws coming within section 1178(a)(2)(B) are preempted if not more stringent, while if a contrary state law comes within section 1178(b) or section 1178(c), it is not preempted. These latter statutory provisions operate by their own terms. Thus, it is not within the Secretary's authority to establish the determination process which these comments seek.

With respect to the request seeking advisory opinions in the section 1178(b) and 1178(c) situations, we agree that we have the authority to issue such opinions. However, the considerations described above that have led us not to adopt a formal process for issuing advisory opinions in the privacy context apply with equal force and effect here.

Comment: One commenter argued that it would be unnecessarily burdensome for state health data agencies (whose focus is on the cost of healthcare or improving Medicare, Medicaid, or the healthcare system) to obtain a specific determination from the Department for an exception under proposed § 160.203(c). States should be required only to notify the Secretary of their own determination that such collection is necessary. It was also argued that cases where the statutory carve-outs apply should not require a Secretarial determination.

Response: We clarify that no Secretarial determination is required for activities that fall into one of the statutory carve-outs. With respect to data collections for state health data agencies, we note that provision has been made for many of these activities in several provisions of the rules below, such as the provisions relating to disclosures required by law (§ 164.512(a)), disclosures for oversight (§ 164.512(d)), and disclosures for public health (§ 164.512(b)). Some disclosures for Medicare and Medicaid purposes may also come within the definition of health care operations. A fuller discussion of this issue appears in connection with § 164.512 below.

Constitutional Comments and Responses

Comment: Several commenters suggested that as a general matter the rule is unconstitutional.

Response: We disagree that the rule is unconstitutional. The particular grounds for this conclusion are set out with respect to particular constitutional issues in the responses below. With respect to the comments that simply made this general assertion, the lack of detail of the comments makes a substantive response impossible.

Article II

Comment: One commenter contended that the Secretary improperly delegated authority to private entities by requiring covered entities to enter into contracts with, monitor, and take action for violations of the contract against their business partners. These comments assert that the selection of these entities to ''enforce'' the regulations violates the Executive Powers Clause and the Appointments and Take Care Clauses.

Response: We reject the assertion that the business associate provisions constitute an improper delegation of executive power to private entities. HIPAA provides HHS with authority to enforce the regulation against covered entities. The rules below regulate only the conduct of the covered entity; to the extent a covered entity chooses to conduct its funding through a business associate, those functions are still functions of the covered entity. Thus, no improper delegation has occurred because what is being regulated are the actions of the covered entity, not the actions of the business associate in its independent capacity.

We also reject the suggestion that the business associates provisions constitute an improper appointment of covered entities to enforce the regulation and violate the Take Care Clause. Because the Secretary has not delegated authority to covered entities, the inference that she has appointed covered entities to exercise such authority misses the mark.

Commerce Clause

Comment: A few commenters suggested that the privacy regulation regulates activities that are not in interstate commerce and which are, therefore, beyond the powers the U.S. Constitution gives the federal government.

Response: We disagree. Health care providers, health plans, and health care clearinghouses are engaged in economic and commercial activities, including the exchange of individually identifiable health information electronically across state lines. These activities constitute interstate commerce. Therefore, they come within the scope of Congress' power to regulate interstate commerce.

Nondelegation Doctrine

Comment: Some commenters objected to the manner by which Congress provided the Secretary authority to promulgate this regulation. These comments asserted that Congress violated the nondelegation doctrine by (1) not providing an ''intelligible principle'' to guide the agency, (2) not

establishing ''ascertainable standards,'' and (3) improperly permitting the Secretary to make social policy decisions.

Response: We disagree. HIPAA clearly delineates Congress' general policy to establish strict privacy protections for individually identifiable health information to encourage electronic transactions. Congress also established boundaries limiting the Secretary's authority. Congress established these limitations in several ways, including by calling for privacy standards for ''individually identifiable health information''; specifying that privacy standards must address individuals' rights regarding their individually identifiable health information, the procedures for exercising those rights, and the particular uses and disclosures to be authorized or required; restricting the direct application of the privacy standards to ''covered entities,'' which Congress defined; requiring consultation with the National Committee on Vital and Health Statistics and the Attorney General; specifying the circumstances under which the federal requirements would supersede state laws; and specifying the civil and criminal penalties the Secretary could impose for violations of the regulation. These limitations also serve as ''ascertainable standards'' upon which reviewing courts can rely to determine the validity of the exercise of authority.

Although Congress could have chosen to impose expressly an exhaustive list of specifications that must be met in order to achieve the protective purposes of the HIPAA, it was entirely permissible for Congress to entrust to the Secretary the task of providing these specifications based on her experience and expertise in dealing with these complex and technical matters.

We disagree with the comments that Congress improperly delegated Congressional policy choices to her. Congress clearly decided to create federal standards protecting the privacy of ''individually identifiable health information'' and not to preempt state laws that are more stringent. Congress also determined over whom the Secretary would have authority, the type of information protected, and the minimum level of regulation.

Separation of Powers

Comment: Some commenters asserted that the federal government may not preempt state laws that are not as strict as the privacy regulation because to do so would violate the separation of powers in the U.S. Constitution. One comment suggested that the rules raised a substantial constitutional issue because, as proposed, they permitted the Secretary to make determinations on preemption, which is a role reserved for the judiciary.

Response: We disagree. We note that this comment only pertains to determinations under section 1178(a)(2)(A); as discussed above, the rules below provide for no Secretarial determinations with respect to state privacy laws coming within section 1178(a)(2)(B). With respect to determinations under section 1178(a)(2)(A), however, the final rules, like the proposed rules, provide that at a state's request the Secretary may make certain determinations regarding the preemptive effect of the rules on a particular state law. As usually the case with any administrative decisions, these are subject to judicial review pursuant to the Administrative Procedure Act.

First Amendment

Comment: Some comments suggested that the rules violated the First Amendment. They asserted that if the rule included Christian Science practitioners as covered entities it would violate the separation of church and state doctrine.

Response: We disagree. The First Amendment does not always prohibit the federal government from regulating secular activities of religious organizations. However, we address concerns relating to Christian Science practitioners more fully in the response to comments discussion of the definition of ''covered entity'' in § 160.103.

Fourth Amendment

Comment: Many comments expressed Fourth Amendment concerns about various proposed provisions. These comments fall into two categories—general concerns about warrantless searches and specific concerns about administrative searches. Several comments argued that the proposed regulations permit law enforcement and government officials access to protected health information without first requiring a judicial search warrant or an individual's consent. These comments rejected the applicability of any of the existing exceptions permitting warrantless searches in this context. Another comment argued that federal and state police should be able to obtain personal medical records only with the informed consent of an individual. Many of these comments also expressed concern that protected health information could be provided to government or private agencies for inclusion in a governmental health data system.

Response: We disagree that the provisions of these rules that permit disclosures for law enforcement purposes and governmental health data systems generally violate the Fourth Amendment. The privacy regulation does not create new access rights for law enforcement. Rather, it refrains from placing a significant barrier in front of access rights that law enforcement currently has under existing legal authority. While the regulation may permit a covered entity to make disclosures in specified instances, it does not require the covered entity make the disclosure. Thus, because we are not modifying existing law regarding disclosures to law enforcement officials, except to strengthen the requirements related to requests already authorized under law, and are not requiring any such disclosures, the privacy regulation does not infringe upon individual's Fourth Amendment rights. We discuss the rationale underlying the permissible disclosures to law enforcement officials more fully in the preamble discussion relating to § 164.512(f).

We note that the proposed provision relating to disclosures to government health data systems has been eliminated in the final rule. However, to the extent that the comments can be seen as raising concern over disclosure of protected health information to government agencies for public health, health oversight, or other purposes permitted by the final rule, the reasoning in the previous paragraph applies.

Comment: One commenter suggested that the rules violate the Fourth Amendment by requiring covered entities to provide access to the Secretary to their books, records, accounts, and facilities to ensure compliance with these rules. The commenter also suggested that the requirement that covered entities enter into agreements with their business partners to make their records available to the Secretary for inspection as well also violates the warrant requirement of the Fourth Amendment.

Response: We disagree. These requirements are consistent with U.S. Supreme Court cases holding that warrantless administrative searches of commercial property are not per se violations of the Fourth Amendment. The provisions requiring that covered entities provide access to certain material to determine compliance with the regulation come within the well-settled exception regarding closely regulated businesses and industries to the warrant requirement. From state and local licensure laws to the federal fraud and abuse statutes and regulations, the health care industry is one of the most

tightly regulated businesses in the country. Because the industry has such an extensive history of government oversight and involvement, those operating within it have no reasonable expectation of privacy from the government such that a warrant would be required to determine compliance with the rules.

In addition, the cases cited by the commenters concern unannounced searches of the premises and facilities of particular entities. Because our enforcement provisions only provide for the review of books, records, and other information and only during normal business hours with notice, except for exceptional situations, this case law does not apply.

As for business associates, they voluntarily enter into their agreements with covered entities. This agreement, therefore, functions as knowing and voluntary consents to the search (even assuming it could be understood to be a search) and obviates the need for a warrant.

Fifth Amendment

Comment: Several comments asserted that the proposed rules violated the Fifth Amendment because in the commenters' views they authorized the taking of privacy property without just compensation or due process of law.

Response: We disagree. The rules set forth below do not address the issue of who owns an individual's medical record. Instead, they address what uses and disclosures of protected health information may be made by covered entities with or without a consent or authorization. As described in response to a similar comment, medical records have been the property of the health care provider or medical facility that created them, historically. In some states, statutes directly provide these entities with ownership. These laws are limited by laws that provide patients or their representatives with access to the records or that provide the patient with an ownership interest in the information within the records. As we discuss, the final rule is consistent with current state law that provides patients access to protected health information, but not ownership of medical records. State laws that provide patients with greater access would remain in effect. Therefore, because patients do not own their records, no taking can occur. As for their interest in the information, the final rule retains their rights. As for covered entities, the final rule does not take away their ownership rights or make their ownership interest in the protected health information worthless. Therefore, no taking has occurred in these situations either.

Ninth and Tenth Amendments

Comment: Several comments asserted that the proposed rules violated the Ninth and Tenth Amendments. One commenter suggested that the Ninth Amendment prohibits long and complicated regulations. Other commenters suggested that the proposed rules authorized the compelled disclosure of individually identifiable health information in violation of State constitutional provisions, such as those in California and Florida. Similarly, a couple of commenters asserted that the privacy rules violate the Tenth Amendment.

Response: We disagree. The Ninth and Tenth Amendments address the rights retained by the people and acknowledge that the States or the people are reserved the powers not delegated to the federal government and not otherwise prohibited by the Constitution. Because HHS is regulating under a delegation of authority from Congress in an area that affects interstate commerce, we are within the powers provided to Congress in the Constitution. Nothing in the Ninth Amendment, or any other provision of the Constitution, restricts the length or complexity of any law. Additionally, we do not believe the rules below impermissibly authorize behavior that violates State constitutions. This rule requires disclosure only to the individual or to the Secretary to enforce this rule. As noted in the preamble discussion of ''Preemption,'' these rules do not preempt State laws, including constitutional provisions, that are contrary to and more stringent, as defined at § 160.502, than these rules. See the discussion of ''Preemption'' for further clarification. Therefore, if these State constitutions are contrary to the rule below and provide greater protection, they remain in full force; if they do not, they are preempted, in accordance with the Supremacy Clause of the Constitution.

Right to Privacy

Comment: Several comments suggested that the proposed regulation would violate the right to privacy guaranteed by the First, Fourth, Fifth, and Ninth Amendments because it would permit covered entities to disclose protected health information without the consent of the individual.

Response: These comments did not provide specific facts or legal basis for the claims. We are, thus, unable to provide a substantive response to these particular comments. However, we note that the rule requires disclosures only to the individual or to the Secretary to determine compliance with this rule. Other uses or disclosures under this rule are permissive, not required. Therefore, if a particular use or disclosure under this rule is viewed as interfering with a right that prohibited the use or disclosure, the rule itself is not what requires the use or disclosure.

Void for Vagueness

Comment: One comment suggested that the Secretary's use of a ''reasonableness'' standard is unconstitutionally vague. Specifically, this comment objected to the requirement that covered entities use ''reasonable'' efforts to use or disclose the minimum amount of protected health information, to ensure that business partners comply with the privacy provisions of their contracts, to notify business partners of any amendments or corrections to protected health information, and to verify the identity of individuals requesting information, as well as charge only a ''reasonable'' fee for inspecting and copying health information. This comment asserted that the Secretary provided ''inadequate guidance'' as to what qualifies as ''reasonable.''

Response: We disagree with the comment's suggestion that by applying a ''reasonableness'' standard, the regulation has failed to provide for ''fair warning'' or ''fair enforcement.'' The ''reasonableness'' standard is well-established in law; for example, it is the foundation of the common law of torts. Courts also have consistently held as constitutional statutes that rely upon a ''reasonableness'' standard. Our reliance upon a ''reasonableness'' standard, thus, provides covered entities with constitutionally sufficient guidance.

Criminal Intent

Comment: One comment argued that the regulation's reliance upon a ''reasonableness'' standard criminalizes ''unreasonable efforts'' without requiring criminal intent or *mens rea.*

Response: We reject this suggestion because HIPAA clearly provides the criminal intent requirement. Specifically, HIPPA provides that a ''person who knowingly and in violation of this part—(1) uses or causes to be used a unique health identifier; (2) obtains individually identifiable health information relating to an individual; or (3) discloses individually identifiable health information to another person, shall be punished as provided in subsection (b).'' HIPAA section 1177 (emphasis added). Subsection (b) also relies on a knowledge standard in

outlining the three levels of criminal sanctions. Thus, Congress, not the Secretary, established the *mens rea* by including the term ''knowingly'' in the criminal penalty provisions of HIPAA.

Data Collection

Comment: One commenter suggested that the U.S. Constitution authorized the collection of data on individuals only for the purpose of the census.

Response: While it might be true that the U.S. Constitution expressly discusses the national census, it does not forbid federal agencies from collecting data for other purposes. The ability of agencies to collect non-census data has been upheld by the courts.

Relationship to Other Federal Laws

Comment: We received several comments that sought clarification of the interaction of various federal laws and the privacy regulation. Many of these comments simply listed federal laws and regulations with which the commenter currently must comply. For example, commenters noted that they must comply with regulations relating to safety, public health, and civil rights, including Medicare and Medicaid, the Americans with Disabilities Act, the Family and Medical Leave Act, the Federal Aviation Administration regulations, the Department of Transportation regulations, the Federal Highway Administration regulations, the Occupational Safety and Health Administration regulations, and the Environmental Protection Agency regulations, and alcohol and drug free workplace rules. These commenters suggested that the regulation state clearly and unequivocally that uses or disclosures of protected health information for these purposes were permissible. Some suggested modifying the definition of health care operations to include these uses specifically. Another suggestion was to add a section that permitted the transmission of protected health information to employers when reasonably necessary to comply with federal, state, or municipal laws and regulations, or when necessary for public or employee safety and health.

Response: Although we sympathize with entities' needs to evaluate the existing laws with which they must comply in light of the requirements of the final regulation, we are unable to respond substantially to comments that do not pose specific questions. We offer, however, the following guidance: if an covered entity is required to disclose protected health information pursuant to a specific statutory or regulatory scheme, the covered entity generally will be permitted under § 164.512(a) to make these disclosures without a consent or authorization; if, however, a statute or regulation merely suggests a disclosure, the covered entity will need to determine if the disclosure comes within another category of permissible disclosure under §§ 164.510 or 164.512 or, alternatively, if the disclosure would otherwise come within § 164.502. If not, the entity will need to obtain a consent or authorization for the disclosure.

Comment: One commenter sought clarification as to when a disclosure is considered to be ''required'' by another law versus ''permitted'' by that law.

Responses: We use these terms according to their common usage. By ''required by law,'' we mean that a covered entity has a legal obligation to disclose the information. For example, if a statute states that a covered entity must report the names of all individuals presenting with gun shot wounds to the emergency room or else be fined $500 for each violation, a covered entity would be required by law to disclose the protected health information necessary to comply with this mandate. The privacy regulation permits this type of disclosure, but does not require it. Therefore, if a covered entity chose not to comply with the reporting statute it would violate only the reporting statute and not the privacy regulation.

On the other hand, if a statute stated that a covered entity may or is permitted to report the names of all individuals presenting with gun shot wounds to the emergency room and, in turn, would receive $500 for each month it made these reports, a covered entity would not be permitted by § 164.512(a) to disclose the protected health information. Of course, if another permissible provision applied to these facts, the covered entity could make the disclosure under that provision, but it would not be considered to be a disclosure. See discussion under § 164.512(a) below.

Comment: Several commenters suggested that the proposed rule was unnecessarily duplicative of existing regulations for federal programs, such as Medicare, Medicaid, and the Federal Employee Health Benefit Program.

Response: Congress specifically subjected certain federal programs, including Medicare, Medicaid, and the Federal Employee Health Benefit Program to the privacy regulation by including them within the definition of ''health plan.'' Therefore, covered entities subject to requirements of existing federal programs will also have to comply with the privacy regulation.

Comment: One comment asserts that the regulation would not affect current federal requirements if the current requirements are weaker than the requirements of the privacy regulation. This same commenter suggested that current federal requirements will trump both state law and the proposed regulation, even if Medicaid transactions remain wholly intrastate.

Response: We disagree. As noted in our discussion of ''Relationship to Other Federal Laws,'' each law or regulation will need to be evaluated individually. We similarly disagree with the second assertion made by the commenter. The final rule will preempt state laws only in specific instances. For a more detailed analysis, see the preamble discussion of ''Preemption.''

Administrative Subpoenas

Comment: One comment stated that the final rule should not impose new standards on administrative subpoenas that would conflict with existing laws or administrative or judicial rules that establish standards for issuing subpoenas. Nor should the final rule conflict with established standards for the conduct of administrative, civil, or criminal proceedings, including the rules regarding the discovery of evidence. Other comments sought further restrictions on access to protected health information in this context.

Response: Section 164.512(e) below addresses disclosures for judicial and administrative proceedings. The final rules generally do not interfere with these existing processes to the extent an individual served with a subpoena, court order, or other similar process is able to raise objections already available. See the discussion below under § 164.512(e) for a fuller response.

Americans with Disabilities Act

Comment: Several comments discussed the intersection between the proposed Privacy Rule and the Americans with Disabilities Act (''ADA'') and sections 503 and 504 of the Rehabilitation Act of 1973. One comment suggested that the final rule explicitly allows disclosures authorized by the Americans with Disabilities Act without an individual's authorization, because this law, in the commenter's view, provides more than adequate protection for the confidentiality of medical records in the employment context. The comment noted that under these laws employers may receive information related to fitness for duty, pre-employment physicals, routine examinations, return to work examinations, examinations following other types of absences, examinations triggered by specific events, changes in

circumstances, requests for reasonable accommodations, leave requests, employee wellness programs, and medical monitoring.

Other commenters suggested that the ADA requires the disclosure of protected health information to employers so that the employee may take advantage of the protections of these laws. They suggested that the final rules clarify that employment may be conditioned on obtaining an authorization for disclosure of protected health information for lawful purposes and provide guidance concerning the interaction of the ADA with the final regulation's requirements. Several commenters wanted clarification that the privacy regulation would not permit employers to request or use protected health information in violation of the ADA.

Response: We disagree with the comment that the final rule should allow disclosures of protected health information authorized by the ADA without the individual's authorization. We learned from the comments that access to and use of protected health information by employers is of particular concern to many people. With regard to employers, we do not have statutory authority to regulate them. Therefore, it is beyond the scope of this regulation to prohibit employers from requesting or obtaining protected health information. Covered entities may disclose protected health information about individuals who are members of an employer's workforce with an authorization. Nothing in the privacy regulation prohibits employers from obtaining that authorization as a condition of employment. We note, however, that employers must comply with other laws that govern them, such as nondiscrimination laws. For example, if an employer receives a request for a reasonable accommodation, the employer may require reasonable documentation about the employee's disability and the functional limitations that require the reasonable accommodation, if the disability and the limitations are not obvious. If the individual provides insufficient documentation and does not provide the missing information in a timely manner after the employer's subsequent request, the employer may require the individual to go to an appropriate health professional of the employer's choice. In this situation, the employee does not authorize the disclosure of information to substantiate the disability and the need for reasonable accommodation, the employer need not provide the accommodation.

We agree that this rule does not permit employers to request or use protected health information in violation of the ADA or other antidiscrimination laws.

Appropriations Laws

Comment: One comment suggested that the penalty provisions of HIPAA, if extended to the privacy regulation, would require the Secretary to violate ''Appropriations Laws'' because the Secretary could be in the position of assessing penalties against her own and other federal agencies in their roles as covered entities. Enforcing penalties on these entities would require the transfer of agency funds to the General Fund.

Response: We disagree. Although we anticipate achieving voluntary compliance and resolving any disputes prior to the actual assessment of penalties, the Department of Justice's Office of Legal Counsel has determined in similar situations that federal agencies have authority to assess penalties against other federal agencies and that doing so is not in violation of the Anti-Deficiency Act, 31 U.S.C. 1341.

Balanced Budget Act of 1997

Comment: One comment expressed concern that the regulation would place tremendous burdens on providers already struggling with the effects of the Balanced Budget Act of 1997.

Response: We appreciate the costs covered entities face when complying with other statutory and regulatory requirements, such as the Balanced Budget Act of 1997. However, HHS cannot address the impact of the Balanced Budget Act or other statutes in the context of this regulation.

Comment: Another comment stated that the regulation is in direct conflict with the Balanced Budget Act of 1997 (''BBA''). The comment asserts that the regulation's compliance date conflicts with the BBA, as well as Generally Acceptable Accounting Principles. According to the comment, covered entities that made capital acquisitions to ensure compliance with the year 2000 (''Y2K'') problem would not be able to account for the full depreciation of these systems until 2005. Because HIPAA requires compliance before that time, the regulation would force premature obsolescence of this equipment because while it is Y2K compliant, it may be HIPAA non-compliant.

Response: This comment raises two distinct issues—(1) the investment in new equipment and (2) the compliance date. With regard to the first issue, we reject the comment's assertion that the regulation requires covered entities to purchase new information systems or information technology equipment, but realize that some covered entities may need to update their equipment. We have tried to minimize the costs, while responding appropriately to Congress' mandate for privacy rules. We have dealt with the cost issues in detail in the ''Regulatory Impact Analysis'' section of this Preamble. With regard to the second issue, Congress, not the Secretary, established the compliance data at section 1175(b) of the Act.

Civil Rights of Institutionalized Persons Act

Comment: A few comments expressed concern that the privacy regulation would inadvertently hinder the Department of Justice Civil Rights Divisions' investigations under the Civil Rights of Institutionalized Persons Act (''CRIPA''). These comments suggested clearly including civil rights enforcement activities as health care oversight.

Response: We agree with this comment. We do not intend for the privacy rules to hinder CRIPA investigations. Thus, the final rule includes agencies that are authorized by law to ''enforce civil rights laws for which health information is relevant'' in the definition of ''health oversight agency'' at § 164.501. Covered entities are permitted to disclose protected health information to health oversight agencies under § 164.512(d) without an authorization. Therefore, we do not believe the final rule should hinder the Department of Justice's ability to conduct investigations pursuant to its authority in CRIPA.

Clinical Laboratory Improvement Amendments

Comment: One comment expressed concern that the proposed definition of health care operations did not include activities related to the quality control clinical studies performed by laboratories to demonstrate the quality of patient test results. Because the Clinical Laboratory Improvement Amendments of 1988 (''CLIA'') requires these studies that the comment asserted require the use of protected health information, the comment suggested including this specific activity in the definition of ''health care operations.''

Response: We do not intend for the privacy regulation to impede the ability of laboratories to comply with the requirements of CLIA. Quality control activities come within the definition of ''health care operations'' in § 164.501 because they come within the meaning of the term ''quality assurance activities.'' To the extent they would not come within health care operations, but

are required by CLIA, the privacy regulation permits clinical laboratories that are regulated by CLIA to comply with mandatory uses and disclosures of protected health information pursuant to § 164.512(a).

Comment: One comment stated that the proposed regulation's right of access for inspection and copying provisions were contrary to CLIA in that CLIA permits laboratories to disclose lab test results only to ''authorized persons.'' This comment suggested that the final rule include language adopting this restriction to ensure that patients not obtain laboratory test results before the appropriate health care provider has reviewed and explained those results to the patients.

A similar comment stated that the lack of preemption of state laws could create problems for clinical laboratories under CLIA. Specifically, this comment noted that CLIA permits clinical laboratories to perform tests only upon the written or electronic request of, and to provide the results to, an ''authorized person.'' State laws define who is an ''authorized person.'' The comment expressed concern as to whether the regulation would preempt state laws that only permit physicians to receive test results.

Response: We agree that CLIA controls in these cases. Therefore, we have amended the right of access, § 164.524(a), so that a covered entity that is subject to CLIA does not have to provide access to the individual to the extent such access would be prohibited by law. Because of this change, we believe the preemption concern is moot.

Controlled Substance Act

Comment: One comment expressed concern that the privacy regulation as proposed would restrict the Drug Enforcement Agency's (''the DEA'') enforcement of the Controlled Substances Act (''CSA''). The comment suggested including enforcement activities in the definition of ''health oversight agency.''

Response: In our view, the privacy regulation should not impede the DEA's ability to enforce the CSA. First, to the extent the CSA requires disclosures to the DEA, these disclosures would be permissible under § 164.512(a). Second, some of the DEA's CSA activities come within the exception for health oversight agencies which permits disclosures to health oversight agencies for:

> Activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections * * * civil, administrative, or criminal proceedings or actions; and other activity necessary for appropriate oversight of the health care system.

Therefore, to the extent the DEA is enforcing the CSA, disclosures to it in its capacity as a health oversight agency are permissible under § 164.512(d). Alternatively, CSA required disclosures to the DEA for law enforcement purposes are permitted under § 164.512(f). When acting as a law enforcement agency under the CSA, the DEA may obtain the information pursuant to § 164.512(f). Thus, we do not agree that the privacy regulation will impede the DEA's enforcement of the CSA. See the preamble discussion of § 164.512 for further explanation.

Comment: One commenter suggested clarifying the provisions allowing disclosures that are ''required by law'' to ensure that the mandatory reporting requirements the CSA imposes on covered entities, including making available reports, inventories, and records of transactions, are not preempted by the regulation.

Response: We agree that the privacy regulation does not alter covered entities' obligations under the CSA. Because the CSA requires covered entities manufacturing, distributing, and/or dispensing controlled substances to maintain and provide to the DEA specific records and reports, the privacy regulation permits these disclosures under § 164.512(a). In addition, when the DEA seeks documents to determine an entity's compliance with the CSA, such disclosures are permitted under § 164.512(d).

Comment: The same commenter expressed concern that the proposed privacy regulation inappropriately limits voluntary reporting and would prevent or deter employees of covered entities from providing the DEA with information about violations of the CSA.

Response: We agree with the general concerns expressed in this comment. We do not believe the privacy rules will limit voluntary reporting of violations of the CSA. The CSA requires certain entities to maintain several types of records that may include protected health information. Although reports that included protected health information may be restricted under these rules, reporting the fact that an entity is not maintaining proper reports is not. If it were necessary to obtain protected health information during the investigatory stages following such a voluntary report, the DEA would be able to obtain the information in other ways, such as by following the administrative procedures outlined in § 164.512(e).

We also agree that employees of covered entities who report violations of the CSA should not be subjected to retaliation by their employers. Under § 164.502(j), we specifically state that a covered entity is not considered to have violated the regulation if a workforce member or business associate in good faith reports violations of laws or professional standards by covered entities to appropriate authorities. See discussion of § 164.502(j) below.

Department of Transportation

Comment: Several commenters stated that the Secretary should recognize in the preamble that it is permissible for employers to condition employment on an individual's delivering a consent to certain medical tests and/or examinations, such as drug-free workplace programs and Department of Transportation (''DOT'')-required physical examinations. These comments also suggested that employers should be able to receive certain information, such as pass/fail test and examination results, fitness-to-work assessments, and other legally required or permissible physical assessments without obtaining an authorization. To achieve this goal, these comments suggested defining ''health information'' to exclude information such as information about how much weight a specific employee can lift.

Response: We reject the suggestion to define ''health information,'' which Congress defined in HIPAA, so that it excludes individually identifiable health information that may be relevant to employers for these types of examinations and programs. We do not regulate employers. Nothing in the rules prohibit employers from conditioning employment on an individual signing the appropriate consent or authorization. By the same token, however, the rules below do not relieve employers from their obligations under the ADA and other laws that restrict the disclosure of individually identifiable health information.

Comment: One commenter asserted that the proposed regulation conflicts with the DOT guidelines regarding positive alcohol and drug tests that require the employer be notified in writing of the results. This document contains protected health information. In addition, the treatment center records must be provided to the Substance Abuse Professional (''SAP'') and the employer must receive a report from SAP with random drug testing recommendations.

Response: It is our understanding that DOT requires drug testing of all applicants for employment in safety-sensitive positions or individuals being transferred to such positions.

Employers, pursuant to DOT regulations, may condition an employee's employment or position upon first obtaining an authorization for the disclosure of results of these tests to the employer. Therefore, we do not believe the final rules conflict with the DOT requirements, which do not prohibit obtaining authorizations before such information is disclosed to employers.

Developmental Disabilities Act

Comment: One commenter urged HHS to ensure that the regulation would not impede access to individually identifiable health information to entities that are part of the Protection and Advocacy System to investigate abuse and neglect as authorized by the Developmental Disabilities Bill of Rights Act.

Response: The Developmental Disabilities Assistance and Bill of Rights Act of 2000 (''DD Act'') mandates specific disclosures of individually identifiable health information to Protection and Advocacy systems designated by the chief elected official of the states and Territories. Therefore, covered entities may make these disclosures under § 164.512(a) without first obtaining an individual's authorization, except in those circumstances in which the DD Act requires the individual's authorization. Therefore, the rules below will not impede the functioning of the existing Protection and Advocacy System.

Employee Retirement Income Security Act of 1974

Comment: Several commenters objected to the fact that the NPRM did not clarify the scope of preemption of state laws under the Employee Retirement Income Security Act of 1974 (ERISA). These commenters asserted that the final rule must state that ERISA preempts all state laws (including those relating to the privacy of individually identifiable health information) so that multistate employers could continue to administer their group health plans using a single set of rules. In contrast, other commenters criticized the Department for its analysis of the current principles governing ERISA preemption of state law, pointing out that the Department has no authority to interpret ERISA.

Response: This Department has no authority to issue regulations under ERISA as requested by some of these commenters, so the rule below does not contain the statement requested. See the discussion of this point under ''Preemption'' above.

Comment: One commenter requested that the final rule clarify that section 264(c)(2) of HIPAA does not save state laws that would otherwise be preempted by the Federal Employees Health Benefits Program. The commenter noted that in the NPRM this statement was made with respect to Medicare and ERISA, but not the law governing the FEHBP.

Response: We agree with this comment. The preemption analysis set out above with respect to ERISA applies equally to the Federal Employees Health Benefit Program.

Comment: One commenter noted that the final rule should clarify the interplay between state law, the preemption standards in Subtitle A of Title I of HIPAA (Health Care Access, Portability and Renewability), and the preemption standards in the privacy requirements in Subtitle F of Title II of HIPAA (Administrative Simplification).

Response: The NPRM described only the preemption standards that apply with respect to the statutory provisions of HIPAA that were implemented by the proposed rule. We agree that the preemption standards in Subtitle A of Title I of HIPAA are different. Congress expressly provided that the preemption provisions of Title I apply only to Part 7, which addresses portability, access, and renewability requirements for Group Health Plans. To the extent state laws contain provisions regarding portability, access, or renewability, as well as privacy requirements, a covered entity will need to evaluate the privacy provisions under the Title II preemption provisions, as explained in the preemption provisions of the rules, and the other provisions under the Title I preemption requirements.

European Union Privacy Directive and U.S. Safe Harbors

Comment: Several comments stated that the privacy regulation should be consistent with the European Union's Directive on Data Protection. Others sought guidance as to how to comply with both the E.U. Directive on Data Protection and the U.S. Safe Harbor Privacy Principles.

Response: We appreciate the need for covered entities obtaining personal data from the European Union to understand how the privacy regulation intersects with the Data Protection Directive. We have provided guidance as to this interaction in the ''Other Federal Laws'' provisions of the preamble.

Comment: A few comments expressed concern that the proposed definition of ''individual'' excluded foreign military and diplomatic personnel and their dependents, as well as overseas foreign national beneficiaries. They noted that the distinctions are based on nationality and are inconsistent with the stance of the E.U. Directive on Data Protection and the Department of Commerce's assurances to the European Commission.

Response: We agree with the general principle that privacy protections should protect every person, regardless of nationality. As noted in the discussion of the definition of ''individual,'' the final regulation's definition does not exclude foreign military and diplomatic personnel, their dependents, or overseas foreign national beneficiaries from the definition of individual. As described in the discussion of § 164.512 below, the final rule applies to foreign diplomatic personnel and their dependents like all other individuals. Foreign military personnel receive the same treatment under the final rule as U.S. military personnel do, as discussed with regard to § 164.512 below. Overseas foreign national beneficiaries to the extent they receive care for the Department of Defense or a source acting on behalf of the Department of Defense remain generally excluded from the final rules protections. For a more detailed explanation, see § 164.500.

Fair Credit Reporting Act

Comment: A few commenters requested that we exclude information maintained, used, or disclosed pursuant to the Fair Credit Reporting Act (''FCRA'') from the requirements of the privacy regulation. These commenters noted that the protection in the privacy regulation duplicate those in the FCRA.

Response: Although we realize that some overlap between FCRA and the privacy rules may exist, we have chosen not to remove information that may come within the purview of FCRA from the scope of our rules because FCRA's focus is not the same as our Congressional mandate to protect individually identifiable health information.

To the extent a covered entity seeks to engage in collection activities or other payment-related activities, it may do so pursuant to the requirements of this rule related to payment. See discussion of §§ 164.501 and 164.502 below.

We understand that some covered entities may be part of, or contain components that are, entities which meet the definition of ''consumer reporting agencies.'' As such, these entities are subject to the FCRA. As described in the preamble to § 164.504, covered entities must designate what parts of their organizations will be treated as covered entities for the

purpose of these privacy rules. The covered entity component will need to comply with these rules, while the components that are consumer reporting agencies will need to comply with FCRA.

Comment: One comment suggested that the privacy regulation would conflict with the FCRA if the regulation's requirement applied to information disclosed to consumer reporting agencies.

Response: To the extent a covered entity is required to disclose protected health information to a consumer reporting agency, it may do so under § 164.512(a). See also discussion under the definition of ''payment'' below.

Fair Debt Collection and Practices Act

Comment: Several comments expressed concern that health plans and health care providers be able to continue using debt collectors in compliance with the Fair Debt Collections Practices Act and related laws.

Response: In our view, health plans and health care providers will be able to continue using debt collectors. Using the services of a debt collector to obtain payment for the provision of health care comes within the definition of ''payment'' and is permitted under the regulation. Thus, so long as the use of debt collectors is consistent with the regulatory requirements (such as, providers obtain the proper consents, the disclosure is of the minimum amount of information necessary to collect the debt, the provider or health plan enter into a business associate agreement with the debt collector, etc.), relying upon debt collectors to obtain reimbursement for the provision of health care would not be prohibited by the regulation.

Family Medical Leave Act

Comment: One comment suggested that the proposed regulation adversely affects the ability of an employer to determine an employee's entitlement to leave under the Family Medical Leave Act (''FMLA'') by affecting the employer's right to receive medical certification of the need for leave, additional certifications, and fitness for duty certification at the end of the leave. The commenter sought clarification as to whether a provider could disclose information to an employer without first obtaining an individual's consent or authorization. Another commenter suggested that the final rule explicitly exclude from the rule disclosures authorized by the FMLA, because, in the commenter's view, it provides more than adequate protection for the confidentiality of medical records in the employment context.

Response: We disagree that the FMLA provides adequate privacy protections for individually identifiable health information. As we understand the FMLA, the need for employers to obtain protected health information under the statute is analogous to the employer's need for protected health information under the ADA. In both situations, employers may need protected health information to fulfill their obligations under these statutes, but neither statute requires covered entities to provide the information directly to the employer. Thus, covered entities in these circumstances will need an individual's authorizations before the disclosure is made to the employer.

Federal Common Law

Comment: One commenter did not want the privacy rules to interfere with the federal common law governing collective bargaining agreements permitting employers to insist on the cooperation of employees with medical fitness evaluations.

Response: We do not seek to interfere with legal medical fitness evaluations. These rules require a covered entity to have an individual's authorization before the information resulting from such evaluations is disclosed to the employer unless another provision of the rule applies. We do not prohibit employers from conditioning employment, accommodations, or other benefits, when legally permitted to do so, upon the individual/employee providing an authorization that would permit the disclosure of protected health information to employers by covered entities. See § 164.508(b)(4) below.

Federal Educational Rights and Privacy Act

Comment: A few commenters supported the exclusion of ''education records'' from the definition of ''protected health information.'' However, one commenter requested that ''treatment records'' of students who are 18 years or older attending post-secondary education institutions be excluded from the definition of ''protected health information'' as well to avoid confusion.

Response: We agree with these commenters. See ''Relationship to Other Federal Laws'' for a description of our exclusion of FERPA ''education records'' and records defined at 20 U.S.C. 1232g(a)(4)(B)(iv), commonly referred to as ''treatment records,'' from the definition of ''protected health information.''

Comment: One comment suggested that the regulation should not apply to any health information that is part of an ''education record'' in any educational agency or institution, regardless of its FERPA status.

Response: We disagree. As noted in our discussion of ''Relationship of Other Federal Laws,'' we exclude education records from the definition of protected health information because Congress expressly provided privacy protections for these records and explained how these records should be treated in FERPA.

Comment: One commenter suggested eliminating the preamble language that describes school nurses and on-site clinics as acting as providers and subject to the privacy regulation, noting that this language is confusing and inconsistent with the statements provided in the preamble explicitly stating that HIPAA does not preempt FERPA.

Response: We agree that this language may have been confusing. We have provided a clearer expression of when schools may be required to comply with the privacy regulation in the ''Relationship to Other Federal Laws'' section of the preamble.

Comment: One commenter suggested adding a discussion of FERPA to the ''Relationship to Other Federal Laws'' section of the preamble.

Response: We agree and have added FERPA to the list of federal laws discussed in ''Relationship to Other Federal Laws'' section of the preamble.

Comment: One commenter stated that school clinics should not have to comply with the ''ancillary'' administrative requirements, such as designating a privacy official, maintaining documentation of their policies and procedures, and providing the Secretary of HHS with access.

Response: We disagree. Because we have excluded education records and records described at 20 U.S.C. 1232g(a)(4)(B)(iv) held by educational agencies and institutions subject to FERPA from the definition of protected health information, only non-FERPA schools would be subject to the administrative requirements. Most of these school clinics will also not be covered entities because they are not engaged in HIPAA transactions and these administrative requirements will not apply to them. However, to the extent a school clinic is within the definition of a health care provider, as Congress defined the term, and the school clinic is engaged in HIPAA transactions, it will be a covered entity and must comply with the rules below.

Comment: Several commenters expressed concern that the privacy regulation would eliminate the parents' ability to have access to information in their children's school health records. Because the proposed regulation suggests that school-based clinics keep health records separate from other educational files, these comments argued that the regulation is contrary to the spirit of FERPA, which provides parents with access rights to their children's educational files.

Response: As noted in the ''Relationship to Other Federal Laws'' provision of the preamble, to the extent information in school-based clinics is not protected health information because it is an education record, the FERPA access requirements apply and this regulation does not. For more detail regarding the rule's application to unemancipated minors, see the preamble discussion about ''Personal Representatives.''

Federal Employees Compensation Act

Comment: One comment noted that the Federal Employees Compensation Act (''FECA'') requires claimants to sign a release form when they file a claim. This commenter suggested that the privacy regulation should not place additional restrictions on this type of release form.

Response: We agree. In the final rule, we have added a new provision, § 164.512(l), that permits covered entities to make disclosures authorized under workers' compensation and similar laws. This provision would permit covered entities to make disclosures authorized under FECA and not require a different release form.

Federal Employees Health Benefits Program

Comment: A few comments expressed concern about the preemption effect on FEHBP and wanted clarification that the privacy regulation does not alter the existing preemptive scope of the program.

Response: We do not intend to affect the preemptive scope of the FEHBP. The Federal Employee Health Benefit Act of 1998 preempts any state law that ''relates to'' health insurance or plans. 5 U.S.C. 8902(m). The final rule does not attempt to alter the preemptive scope Congress has provided to the FEHBP.

Comment: One comment suggested that in the context of FEHBP HHS should place the enforcement responsibilities of the privacy regulation with Office of Personnel Management, as the agency responsible for administering the program.

Response: We disagree. Congress placed enforcement with the Secretary. *See* section 1176 of the Act.

Federal Rules of Civil Procedure

Comment: A few comments suggested revising proposed § 164.510(d) so that it is consistent with the existing discovery procedure under the Federal Rules of Civil Procedure or local rules.

Response: We disagree that the rules regarding disclosures and uses of protected health information for judicial and administrative procedures should provide only those protections that exist under existing discovery rules. Although the current process may be appropriate for other documents and information requested during the discovery process, the current system, as exemplified by the Federal Rules of Civil Procedure, does not provide sufficient protection for protected health information. Under current discovery rules, private attorneys, government officials, and others who develop such requests make the initial determinations as to what information or documentation should be disclosed. Independent third-party review, such as that by a court, only becomes necessary if a person of whom the request is made refuses to provide the information. If this happens, the person seeking discovery must obtain a court order or move to compel discovery. In our view this system does not provide sufficient protections to ensure that unnecessary and unwarranted disclosures of protected health information does not occur. For a related discuss, see the preamble regarding ''Disclosures for Judicial and Administrative Proceedings'' under § 164.512(e).

Federal Rules of Evidence

Comment: Many comments requested clarification that the privacy regulation does not conflict or interfere with the federal or state privileges. In particular, one of these comments suggested that the final regulation provide that disclosures for a purpose recognized by the regulation not constitute a waiver of federal or state privileges.

Response: We do not intend for the privacy regulation to interfere with federal or state rules of evidence that create privileges. Consistent with The Uniform Health-Care Information Act drafted by the National Conference of Commissioners on Uniform State Laws, we do not view a consent or an authorization to function as a waiver of federal or state privileges. For further discussion of the effect of consent or authorization on federal or state privileges, see preamble discussions in §§ 164.506 and 164.508.

Comment: Other comments applauded the Secretary's references to *Jaffee* v. *Redman,* 518 U.S. 1 (1996), which recognized a psychotherapist-patient privilege, and asked the Secretary to incorporate expressly this privilege into the final regulation.

Response: We agree that the psychotherapist-patient relationship is an important one that deserves protection. However, it is beyond the scope our mandate to create specific evidentiary privileges. It is also unnecessary because the United States Supreme Court has adopted this privilege.

Comment: A few comments discussed whether one remedy for violating the privacy regulation should be to exclude or suppress evidence obtained in violation of the regulation. One comment supported using this penalty, while another opposed it.

Response: We do not have the authority to mandate that courts apply or not apply the exclusionary rule to evidence obtained in violation of the regulation. This issue is in the purview of the courts.

Federal Tort Claims Act

Comment: One comment contended that the proposed regulation's requirement mandating covered entities to name the subjects of protected health information disclosed under a business partner contract as third party intended beneficiaries under the contract would have created an impermissible right of action against the government under the Federal Tort Claims Act (''FTCA'').

Response: Because we have deleted the third party beneficiary provisions from the final rules, this comment is moot.

Comment: Another comment suggested the regulation would hamper the ability of federal agencies to disclose protected health information to their attorneys, the Department of Justice, during the initial stages of the claims brought under the FTCA.

Response: We disagree. The regulation applies only to federal agencies that are covered entities. To the extent an agency is not a covered entity, it is not subject to the regulation; to the extent an agency is a covered entity, it must comply with the regulation. A covered entity that is a federal agency may disclose relevant information to its attorneys, who are business associates, for purposes of health care operations, which includes uses or disclosures for legal functions. See § 164.501 (definitions of ''business associate'' and ''health care operations''). The final rule provides specific provisions describing how federal agencies may provide

adequate assurances for these types of disclosures of protected health information. See § 164.504(e)(3).

Food and Drug Administration

Comment: A few comments expressed concerns about the use of protected health information for reporting activities to the Food and Drug Administration (''FDA''). Their concern focused on the ability to obtain or disclose protected health information for pre-and post-marketing adverse event reports, device tracking, and post-marketing safety and efficacy evaluation.

Response: We agree with this comment and have provided that covered entities may disclose protected health information to persons subject to the jurisdiction of the FDA, to comply with the requirements of, or at the direction of, the FDA with regard to reporting adverse events (or similar reports with respect to dietary supplements), the tracking of medical devices, other post-marketing surveillance, or other similar requirements described at § 164.512(b).

Foreign Standards

Comment: One comment asked how the regulation could be enforced against foreign countries (or presumably entities in foreign countries) that solicit medical records from entities in the United States.

Response: We do not regulate solicitations of information. To the extent a covered entity wants to comply with a request for disclosure of protected health information to foreign countries or entities within foreign countries, it will need to comply with the privacy rules before making the disclosure. If the covered entity fails to comply with the rules, it will be subject to enforcement proceedings.

Freedom of Information Act

Comment: One comment asserted that the proposed privacy regulation conflicts with the Freedom of Information Act (''FOIA''). The comment argued that the proposed restriction on disclosures by agencies would not come within one of the permissible exemptions to the FOIA. In addition, the comment noted that only in exceptional circumstances would the protected health information of deceased individuals come within an exemption because, for the most part, death extinguishes an individual's right to privacy.

Response: Section 164.512(a) below permits covered entities to disclose protected health information when such disclosures are required by other laws as long as they follow the requirements of those laws. Therefore, the privacy regulation will not interfere with the ability of federal agencies to comply with FOIA, when it requires the disclosure.

We disagree, however, that most protected health information will not come within Exemption 6 of FOIA. See the discussion above under ''Relationship to Other Federal Laws'' for our review of FOIA. Moreover, we disagree with the comment's assertion that the protected health information of deceased individuals does not come within Exemption 6. Courts have recognized that a deceased individual's surviving relatives may have a privacy interest that federal agencies may consider when balancing privacy interests against the public interest in disclosure of the requested information. Federal agencies will need to consider not only the privacy interests of the subject of the protected health information in the record requested, but also, when appropriate, those of a deceased individual's family consistent with judicial rulings.

If an agency receives a FOIA request for the disclosure of protected health information of a deceased individual, it will need to determine whether or not the disclosure comes within Exemption 6. This evaluation must be consistent with the court's rulings in this area. If the exemption applies, the federal agency will not have to release the information. If the federal agency determines that the exemption does not apply, may release it under § 164.512(a) of this regulation.

Comment: One commenter expressed concern that our proposal to protect the individually identifiable health information about the deceased for two years following death would impede public interest reporting and would be at odds with many state Freedom of Information laws that make death records and autopsy reports public information. The commenter suggested permitting medical information to be available upon the death of an individual or, at the very least, that an appeals process be permitted so that health information trustees would be allowed to balance the interests in privacy and in public disclosure and release or not release the information accordingly.

Response: These rules permit covered entities to make disclosures that are required by state Freedom of Information Act (FOIA) laws under § 164.512(a). Thus, if a state FOIA law designates death records and autopsy reports as public information that must be disclosed, a covered entity may disclose it without an authorization under the rule. To the extent that such information is required to be disclosed by FOIA or other law, such disclosures are permitted under the final rule. In addition, to the extent that death records and autopsy reports are obtainable from non-covered entities, such as state legal authorities, access to this information is not impeded by this rule.

If another law does not require the disclosure of death records and autopsy reports generated and maintained by a covered entity, which are protected health information, covered entities are not allowed to disclose such information except as permitted or required by the final rule, even if another entity discloses them.

Comment: One comment sought clarification of the relationship between the Freedom of Information Act, the Privacy Act, and the privacy rules.

Response: We have provided this analysis in the ''Relationship to Other Federal Laws'' section of the preamble in our discussion of the Freedom of Information Act.

Gramm-Leach-Bliley

Comments: One commenter noted that the Financial Services Modernization Act, also known as Gramm-Leach-Bliley (''GLB''), requires financial institutions to provide detailed privacy notices to individuals. The commenter suggested that the privacy regulation should not require financial institutions to provide additional notice.

Response: We disagree. To the extent a covered entity is required to comply with the notice requirements of GLB and those of our rules, the covered entity must comply with both. We will work with the FTC and other agencies implementing GLB to avoid unnecessary duplication. For a more detailed discussion of GLB and the privacy rules, see the ''Relationship to Other Federal Laws'' section of the preamble.

Comment: A few commenters asked that the Department clarify that financial institutions, such as banks, that serve as payors are covered entities. The comments explained that with the enactment of the Gramm-Leach-Bliley Act, banks are able to form holding companies that will include insurance companies (that may be covered entities). They recommended that banks be held to the rule's requirements and be required to obtain authorization to conduct non-payment activities, such as for the marketing of health and non-health items and services or the use and disclosure to non-health related divisions of the covered entity.

Response: These comments did not provide specific facts that would permit us to provide a substantive response. An organization will need to determine whether it comes within the definition of ''covered entity.'' An organization may also need to consider whether or not it contains a health care component. Organizations that are uncertain about the application of the regulation to them will need to evaluate their specific facts in light of this rule.

Inspector General Act

Comment: One comment requested the Secretary to clarify in the preamble that the privacy regulation does not preempt the Inspector General Act.

Response: We agree that to the extent the Inspector General Act requires uses or disclosures of protected health information, the privacy regulation does not preempt it. The final rule provides that to the extent required under section 201(a)(5) of the Act, nothing in this subchapter should be construed to diminish the authority of any Inspector General, including the authority provided in the Inspector General Act of 1978. See discussion of § 160.102 above.

Medicare and Medicaid

Comment: One comment suggested possible inconsistencies between the regulation and Medicare/Medicaid requirements, such as those under the Quality Improvement System for Managed Care. This commenter asked that HHS expand the definition of health care operations to include health promotion activities and avoid potential conflicts.

Response: We disagree that the privacy regulation would prohibit managed care plans operating in the Medicare or Medicaid programs from fulfilling their statutory obligations. To the extent a covered entity is required by law to use or disclose protected health information in a particular manner, the covered entity may make such a use or disclosure under § 164.512(a). Additionally, quality assessment and improvement activities come within the definition of ''health care operations.'' Therefore, the specific example provided by the commenter would seem to be a permissible use or disclosure under § 164.502, even if it were not a use or disclosure ''required by law.''

Comment: One commenter stated that Medicare should not be able to require the disclosure of psychotherapy notes because it would destroy a practitioner's ability to treat patients effectively.

Response: If the Title XVIII of the Social Security Act requires the disclosure of psychotherapy notes, the final rule permits, but does not require, a covered entity to make such a disclosure under § 164.512(a). If, however, the Social Security Act does not require such disclosures, Medicare does not have the discretion to require the disclosure of psychotherapy notes as a public policy matter because the final rule provides that covered entities, with limited exceptions, must obtain an individual's authorization before disclosing psychotherapy notes. See § 164.508(a)(2).

National Labor Relations Act

Comment: A few comments expressed concern that the regulation did not address the obligation of covered entities to disclose protected health information to collective bargaining representatives under the National Labor Relations Act.

Response: The final rule does not prohibit disclosures that covered entities must make pursuant to other laws. To the extent a covered entity is required by law to disclose protected health information to collective bargaining representatives under the NLRA, it may to so without an authorization. Also, the definition of ''health care operations'' at § 164.501 permits disclosures to employee representatives for purposes of grievance resolution.

Organ Donation

Comment: One commenter expressed concern about the potential impact of the regulation on the organ donation program under 42 CFR part 482.

Response: In the final rule, we add provisions allowing the use or disclosure of protected health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating donation and transplantation. See § 164.512(h).

Privacy Act Comments

Comment: One comment suggested that the final rule unambiguously permit the continued operation of the statutorily established or authorized discretionary routine uses permitted under the Privacy Act for both law enforcement and health oversight.

Response: We disagree. See the discussion of the Privacy Act in ''Relationship to Other Federal Laws'' above.

Public Health Services Act

Comment: One comment suggested that the Public Health Service Act places more stringent rules regarding the disclosure of information on Federally Qualified Health Centers than the proposed privacy regulation suggested. Therefore, the commenter suggested that the final rule exempt Federally Qualified Health Centers from the rules requirements

Response: We disagree. Congress expressly included Federally Qualified Health Centers, a provider of medical or other health services under the Social Security Act section 1861(s), within its definition of health care provider in section 1171 of the Act; therefore, we cannot exclude them from the regulation.

Comment: One commenter noted that no conflicts existed between the proposed rule and the Public Health Services Act.

Response: As we discuss in the ''Relationship to Other Federal Laws'' section of the preamble, the Public Health Service Act contains explicit confidentiality requirements that are so general as not to create problems of inconsistency. We recognized, however, that in some cases, that law or its accompanying regulations may contain greater restrictions. In those situations, a covered entity's ability to make what are permissive disclosures under this privacy regulation would be limited by those laws.

Reporting Requirement

Comment: One comment noted that federal agencies must provide information to certain entities pursuant to various federal statutes. For example, federal agencies must not withhold information from a Congressional oversight committee or the General Accounting Office. Similarly, some federal agencies must provide the Bureau of the Census and the National Archives and Records Administration with certain information. This comment expressed concern that the privacy regulation would conflict with these requirements. Additionally, the commenter asked whether the privacy notice would need to contain these uses and disclosures and recommended that a general statement that these federal agencies would disclose protected health information when required by law be considered sufficient to meet the privacy notice requirements.

Response: To the extent a federal agency acting as a covered entity is required by federal statute to disclose protected health information, the regulation permits the disclosure as required by law under § 164.512(a). The notice provisions at § 164.520(b)(1)(ii)(B) require covered entities to provide a brief description of the purposes for which the covered

entity is permitted or required by the rules to use or disclose protected health information without an individual's written authorization. If these statutes require the disclosures, covered entities subject to the requirement may make the disclosure pursuant to § 164.512(a). Thus, their notice must include a description of the category of these disclosures. For example, a general statement such as the covered entity ''will disclose your protected health information to comply with legal requirements'' should suffice.

Comment: One comment stressed that the final rule should not inadvertently preempt mandatory reporting laws duly enacted by federal, state, or local legislative bodies. This commenter also suggested that the final rule not prevent the reporting of violations to law enforcement agencies.

Response: We agree. Like the proposed rule, the final rule permits covered entities to disclose protected health information when required by law under § 164.512(a). To the extent a covered entity is required by law to make a report to law enforcement agencies or is otherwise permitted to make a disclosure to a law enforcement agency as described in § 164.512(f), it may do so without an authorization. Alternatively, a covered entity may always request that individuals authorize these disclosures.

Security Standards

Comment: One comment called for HHS to consider the privacy regulation in conjunction with the other HIPAA standards. In particular, this comment focused on the belief that the security standards should be compatible with the existing and emerging health care and information technology industry standards.

Response: We agree that the security standards and the privacy rules should be compatible with one another and are working to ensure that the final rules in both areas function together. Because we are addressing comments regarding the privacy rules in this preamble, we will consider the comment about the security standard as we finalize that set of rules.

Substance Abuse Confidentiality Statute and Regulations

Comment: Several commenters noted that many health care providers are bound by the federal restrictions governing alcohol and drug abuse records. One commenter noted that the NPRM differed substantially from the substance abuse regulations and would have caused a host of practical problems for covered entities. Another commenter, however, supported the NPRM's analysis that stated that more stringent provisions of the substance abuse provisions would apply. This commenter suggested an even stronger approach of including in the text a provision that would preserve existing federal law. Yet, one comment suggested that the regulation as proposed would confuse providers by making it difficult to determine when they may disclose information to law enforcement because the privacy regulation would permit disclosures that the substance abuse regulations would not.

Response: We appreciate the need of some covered entities to evaluate the privacy rules in light of federal requirements regarding alcohol and drug abuse records. Therefore, we provide a more detailed analysis in the ''Relationship to Other Federal Laws'' section of the preamble.

Comment: Some of these commenters also noted that state laws contain strict confidentiality requirements. A few commenters suggested that HHS reassess the regulations to avoid inconsistencies with state privacy requirements, implying that problems exist because of conflicts between the federal and state laws regarding the confidentiality of substance abuse information.

Response: As noted in the preamble section discussing preemption, the final rules do not preempt state laws that provide more privacy protections. For a more detailed analysis of the relationship between state law and the privacy rules, see the ''Preemption'' provisions of the preamble.

Tribal Law

Comments: One commenter suggested that the consultation process with tribal governments described in the NPRM was inadequate under Executive Order No. 13084. In addition, the commenter expressed concern that the disclosures for research purposes as permitted by the NPRM would conflict with a number of tribal laws that offer individuals greater privacy rights with respect to research and reflects cultural appropriateness. In particular, the commenter referenced the Health Research Code for the Navajo Nation which creates a entity with broader authority over research conducted on the Navajo Nation than the local IRB and requires informed consent by study participants. Other laws mentioned by the commenter included the Navajo Nation Privacy and Access to Information Act and a similar policy applicable to all health care providers within the Navajo Nation. The commenter expressed concern that the proposed regulation research provisions would override these tribal laws.

Response: We disagree with the comment that the consultation with tribal governments undertaken prior to the proposed regulation is inadequate under Executive Order No. 13084. As stated in the proposed regulation, the Department consulted with representatives of the National Congress of American Indians and the National Indian Health Board, as well as others, about the proposals and the application of HIPAA to the Tribes, and the potential variations based on the relationship of each Tribe with the IHS for the purpose of providing health services. In addition, Indian and tribal governments had the opportunity to, and did, submit substantive comments on the proposed rules.

Additionally, disclosures permitted by this regulation do not conflict with the policies as described by this commenter. Disclosures for research purposes under the final rule, as in the proposed regulation, are permissive disclosures only. The rule describes the outer boundaries of permissible disclosures. A covered health care provider that is subject to the tribal laws of the Navajo Nation must continue to comply with those tribal laws. If the tribal laws impose more stringent privacy standards on disclosures for research, such as requiring informed consent in all cases, nothing in the final rule would preclude compliance with those more stringent privacy standards. The final rule does not interfere with the internal governance of the Navajo Nation or otherwise adversely affect the policy choices of the tribal government with respect to the cultural appropriateness of research conducted in the Navajo Nation.

TRICARE

Comment: One comment expressed concern regarding the application of the ''minimum necessary'' standard to investigations of health care providers under the TRICARE (formerly the CHAMPUS) program. The comment also expressed concern that health care providers would be able to avoid providing their records to such investigators because the proposed § 164.510 exceptions were not mandatory disclosures.

Response: In our view, neither the minimum necessary standard nor the final §§ 164.510 and 164.512 permissive disclosures will impede such investigations. The regulation requires covered entities to make all reasonable efforts not to disclose more than the minimum amount of protected health

information necessary to accomplish the intended purpose of the use or disclosure. This requirement, however, does not apply to uses or disclosures that are required by law. See § 164.502(b)(2)(iv). Thus, if the disclosure to the investigators is required by law, the minimum necessary standard will not apply. Additionally, the final rule provides that covered entities rely, if such reliance is reasonable, on assertions from public officials about what information is reasonably necessary for the purpose for which it is being sought. See § 164.514(d)(3)(iii).

We disagree with the assertion that providers will be able to avoid providing their records to investigators. Nothing in this rule permits covered entities to avoid disclosures required by other laws.

Veterans Affairs

Comment: One comment sought clarification about how disclosures of protected health information would occur within the Veterans Affairs programs for veterans and their dependents.

Response: We appreciate the commenter's request for clarification as to how the rules will affect disclosures of protected health information in the specific context of Veteran's Affairs programs. Veterans health care programs under 38 U.S.C. chapter 17 are defined as ''health plans.'' Without sufficient details as to the particular aspects of the Veterans Affairs programs that this comment views as problematic, we cannot comment substantively on this concern.

Comment: One comment suggested that the final regulation clarify that the analysis applied to the substance abuse regulations apply to laws governing Veteran's Affairs health records.

Response: Although we realize some difference may exist between the laws, we believe the discussion of federal substance abuse confidentiality regulations in the ''Relationship to Other Federal Laws'' preamble provides guidance that may be applied to the laws governing Veteran's Affairs (''VA'') health records. In most cases, a conflict will not exist between these privacy rules and the VA programs. For example, some disclosures allowed without patient consent or authorization under the privacy regulation may not be within the VA statutory list of permissible disclosures without a written consent. In such circumstances, the covered entity would have to abide by the VA statute, and no conflict exists. If the disclosures permitted by the VA statute come within the permissible disclosures of our rules, no conflict exists. In some cases, our rules may demand additional requirements, such as obtaining the approval of a privacy board or Institutional Review Board if a covered entity seeks to disclose protected health information for research purposes without the individual's authorization. A covered entity subject to the VA statute will need to ensure that it meets the requirements of both that statute and the regulation below. If a conflict arises, the covered entity should evaluate the specific potential conflicting provisions under the implied repeal analysis set forth in the ''Relationship to Other Federal Laws'' discussion in the preamble.

WIC

Comment: One comment called on other federal agencies to examine their regulations and policies regarding the use and disclosure of protected health information. The comment suggested that other agencies revise their regulations and policies to avoid duplicative, contradictory, or more stringent requirements. The comment noted that the U.S. Department of Agriculture's Special Supplemental Nutrition Program for Women, Infants, and Children (''WIC'') does not release WIC data. Because the commenter believed the regulation would not prohibit the disclosure of WIC data, the comment stated that the Department of Agriculture should now release such information.

Response: We support other federal agencies to whom the rules apply in their efforts to review existing regulations and policies regarding protected health information. However, we do not agree with the suggestion that other federal agencies that are not covered entities must reduce the protections or access-related rights they provide for individually identifiable health information they hold.

Part 160, Subpart C—Compliance and Enforcement

Section 160.306(a)—Who Can File Complaints With the Secretary

Comment: The proposed rule limited those who could file a complaint with the Secretary to individuals. A number of commenters suggested that other persons with knowledge of a possible violation should also be able to file complaints. Examples that were provided included a mental health care provider with first hand knowledge of a health plan improperly requiring disclosure of psychotherapy notes and an occupational health nurse with knowledge that her human resources manager is improperly reviewing medical records. A few comments raised the concern that permitting any person to file a complaint lends itself to abuse and is not necessary to ensure privacy rights and that the complainant should be a person for whom there is a duty to protect health information.

Response: As discussed below, the rule defines ''individual'' as the person who is the subject of the individually identifiable health information. However, the covered entity may allow other persons, such as personal representatives, to exercise the rights of the individual under certain circumstances, e.g., for a deceased individual. We agree with the commenters that any person may become aware of conduct by a covered entity that is in violation of the rule. Such persons could include the covered entity's employees, business associates, patients, or accrediting, health oversight, or advocacy agencies or organizations. Many persons, such as the covered entity's employees, may, in fact, be in a better position than the ''individual'' to know that a violation has occurred. Another example is a state Protection and Advocacy group that may represent persons with developmental disabilities. We have decided to allow complaints from any person. The term ''person'' is not restricted here to human beings or natural persons, but also includes any type of association, group, or organization.

Allowing such persons to file complaints may be the only way the Secretary may learn of certain possible violations. Moreover, individuals who are the subject of the information may not be willing to file a complaint because of fear of embarrassment or retaliation. Based on our experience with various civil rights laws, such as Title VI of the Civil Rights Act of 1964 and Title II of the Americans with Disabilities Act, that allow any person to file a complaint with the Secretary, we do not believe that this practice will result in abuse. Finally, upholding privacy protections benefits all persons who have or may be served by the covered entity as well as the general public, and not only the subject of the information.

If a complaint is received from someone who is not the subject of protected health information, the person who is the subject of this information may be concerned with the Secretary's investigation of this complaint. While we did not receive comments on this issue, we want to protect the privacy rights of this individual. This might

involve the Secretary seeking to contact the individual to provide information as to how the Secretary will address individual's privacy concerns while resolving the complaint. Contacting all individuals may not be practicable in the case of allegations of systemic violations (e.g., where the allegation is that hundreds of medical records were wrongfully disclosed).

Requiring That a Complainant Exhaust the Covered Entity's Internal Complaint Process Prior to Filing a Complaint With the Secretary

Comment: A number of commenters, primarily health plans, suggested that individuals should not be permitted to file a complaint with the Secretary until they exhaust the covered entity's own complaint process. Commenters stated that covered entities should have a certain period of time, such as ninety days, to correct the violation. Some commenters asserted that providing for filing a complaint with the Secretary will be very expensive for both the public and private sectors of the health care industry to implement. Other commenters suggested requiring the Secretary to inform the covered entity of any complaint it has received and not initiate an investigation or ''take enforcement action'' before the covered entity has time to address the complaint.

Response: We have decided, for a number of reasons, to retain the approach as presented in the proposed rule. First, we are concerned that requiring that complainants first notify the covered entity would have a chilling effect on complaints. In the course of investigating individual complaints, the Secretary will often need to reveal the identity of the complainant to the covered entity. However, in the investigation of cases of systemic violations and some individual violations, individual names may not need to be identified. Under the approach suggested by these commenters, the covered entity would learn the names of all persons who file complaints with the Secretary. Some individuals might feel uncomfortable or fear embarrassment or retaliation revealing their identity to the covered entity they believe has violated the regulation. Individuals may also feel they are being forced to enter into negotiations with this entity before they can file a complaint with the Secretary.

Second, because some potential complainants would not bring complaints to the covered entity, possible violations might not become known to the Secretary and might continue. Third, the delay in the complaint coming to the attention of the Secretary because of the time allowed for the covered entity to resolve the complaint may mean that significant violations are not addressed expeditiously. Finally, the process proposed by these commenters is arguably unnecessary because an individual who believes that an agreement can be reached with the covered entity, can, through the entity's internal complaint process or other means, seek resolution before filing a complaint with the Secretary.

Our approach is consistent with other laws and regulations protecting individual rights. None of the civil rights laws enforced by the Secretary require a complainant to provide any notification to the entity that is alleged to have engaged in discrimination (e.g., Americans with Disabilities Act, section 504 of the Rehabilitation Act, Title VI of the Civil Rights Act, and the Age Discrimination Act). The concept of ''exhaustion'' is used in laws that require individuals to pursue administrative remedies, such as that provided by a governmental agency, before bringing a court action. Under HIPAA, individuals do not have a right to court action.

Some commenters seemed to believe that the Secretary would pursue enforcement action without notifying the covered entity. It has been the Secretary's practice in investigating cases under other laws, such as various civil rights laws, to inform entities that we have received a complaint against them and to seek early resolution if possible. In enforcing the privacy rule, the Secretary will generally inform the covered entity of the nature of any complaints it has received against the entity. (There may be situations where information is withheld to protect the privacy interests of the complainant or others or where revealing information would impede the investigation of the covered entity.) The Secretary will also generally afford the entity an opportunity to share information with the Secretary that may result in an early resolution. Our approach will be to seek informal resolution of complaints whenever possible, which includes allowing covered entities a reasonable amount of time to work with the Secretary to come into compliance before initiating action to seek civil monetary penalties.

Section 160.306(b)(3)—Requiring That Complaints Be Filed With the Secretary Within a Certain Period of Time

Comment: A number of commenters, primarily privacy and disability advocacy organizations, suggested that the regulation require that complaints be filed with the Secretary by a certain time. These commenters generally recommended that the time period for filing a complaint should commence to run from the time when the individual knew or had reason to know of the violation or omission. Another comment suggested that a requirement to file a complaint with the Secretary within 180 days of the alleged noncompliance is a problem because a patient may, because of his or her medical condition, be unable to access his or her records within that time frame.

Response: We agree with the commenters that complainants should generally be required to submit complaints in a timely fashion. Federal regulations implementing Title VI of the Civil Rights Act of 1964 provide that ''[a] complaint must be filed not later than '180 days from the date of the alleged discrimination' unless the time for filing is extended by the responsible Department official or his designee.'' 45 CFR 80.7(b). Other civil rights laws, such as the Age Discrimination Act, section 504 of the Rehabilitation Act, and Title II of the Americans with Disabilities Act (ADA) (state and local government services), also use this approach. Under civil rights laws administered by the EEOC, individuals have 180 days of the alleged discriminatory act to file a charge with EEOC (or 300 days if there is a state or local fair employment practices agency involved).

Therefore, in the final rule we require that complaints be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred unless this time limit is waived by the Secretary for good cause shown. We believe that an investigation of a complaint is likely to be most effective if persons can be interviewed and documents reviewed as close to the time of the alleged violation as possible. Requiring that complaints generally be filed within a certain period of time increases the likelihood that the Secretary will have necessary and reliable information. Moreover, we are taking this approach in order to encourage complainants to file complaints as soon as possible. By receiving complaints in a timely fashion, we can, if such complaints prove valid, reduce the harm caused by the violation.

Section 160.308—Basis for Conducting Compliance Reviews

Comment: A number of comments expressed concern that the Secretary would conduct compliance reviews

without having received a complaint or having reason to believe there is noncompliance. A number of these commenters appeared to believe that the Secretary would engage in ''routine visits.'' Some commenters suggested that the Secretary should only be able to conduct compliance reviews if the Secretary has initiated an investigation of a complaint regarding the covered entity in the preceding twelve months. Some commenters suggested that there should only be compliance reviews based on established criteria for reviews (e.g., finding of ''reckless disregard''). Many of these commenters stated that cooperating with compliance reviews is potentially burdensome and expensive.

One commenter asked whether the Secretary will have a process for reviewing all covered entities to determine how they are complying with requirements. This commenter questioned whether covered entities will be required to submit plans and wait for Departmental approval.

Another commenter suggested that the Secretary specify a time limit for the completion of a compliance review.

Response: We disagree with the commenters that the final rule should restrict the Secretary's ability to conduct compliance reviews. The Secretary needs to maintain the flexibility to conduct whatever reviews are necessary to ensure compliance with the rule.

Section 160.310 (a) and (c)—The Secretary's Access to Information in Determining Compliance

Comment: Some commenters raised objections to provisions in the proposed rule which required that covered entities maintain records and submit compliance reports as the Secretary determines is necessary to determine compliance and required that covered entities permit access by the Secretary during normal business hours to its books, records, accounts, and other sources of information, including protected health information, and its facilities, that are pertinent to ascertaining compliance with this subpart. One commenter stated that the Secretary's access to private health information without appropriate patient consent is contrary to the intent of HIPAA. Another commenter expressed the view that, because covered entities face criminal penalties for violations, these provisions violate the Fifth Amendment protections against forced self incrimination. Other commenters stated that covered entities should be given the reason the Secretary needs to have access to its books and records. Another commenter stated that there should be a limit to the frequency or extent of intrusion by the federal government into the business practices of a covered entity and that these provisions violate the Fourth Amendment of the Constitution.

Finally, a coalition of church plans suggested that the Secretary provide church plans with additional procedural safeguards to reduce unnecessary intrusion into internal church operations. These suggested safeguards included permitting HHS to obtain records and other documents only if they are relevant and necessary to compliance and enforcement activities related to church plans, requiring a senior official to determine the appropriateness of compliance-related activities for church plans, and providing church plans with a self-correcting period similar to that Congress expressly provided in Title I of HIPAA under the tax code.

Response: The final rule retains the proposed language in these two provisions with one change. The rule adds a provision indicating that the Secretary's access to information held by the covered entity may be at any time and without notice where exigent circumstances exist, such as where time is of the essence because documents might be hidden or destroyed. Thus, covered entities will generally receive notice before the Secretary seeks to access the entity's books or records.

Other than the exigent circumstances language, the language in these two provisions is virtually the same as the language in this Department's regulation implementing Title VI of the Civil Rights Act of 1964. 45 CFR 80.6(b) and (c). The Title VI regulation is incorporated by reference in other Department regulations prohibiting discrimination of the basis of disability. 45 CFR 84.61. Similar provisions allowing this Department access to recipient information is found in the Secretary's regulation implementing the Age Discrimination Act. 45 CFR 91.34. These provisions have not proved to be burdensome to entities that are subject to these civil rights regulations (i.e., all recipients of Department funds).

We do not interpret Constitutional case law as supporting the view that a federal agency's review of information pursuant to statutory mandate violates the Fifth Amendment protections against forced self incrimination. Nor would such a review of this information raise Fourth Amendment problems. See discussion above regarding Constitutional comments and responses.

We appreciate the concern that the Secretary not involve herself unnecessarily into the internal operations of church plans. However, by providing health insurance or care to their employees, church plans are engaging in a secular activity. Under the regulation, church plans are subject to the same compliance and enforcement requirements with which other covered entities must comply. Because Congress did not carve out specific exceptions or require stricter standards for investigations related to church plans, incorporating such measures into the regulation would be inappropriate.

Additionally, there is no indication that the regulation will directly interfere with the religious practices of church plans. Also, the regulation as written appropriately limits the ability of investigators to obtain information from covered entities. The regulation provides that the Secretary may obtain access only to information that is pertinent to ascertain compliance with the regulation. We do not anticipate asking for information that is not necessary to assess compliance with the regulation. The purpose of obtaining records and similar materials is to determine compliance, not to engage in any sort of review or evaluation of religious activities or beliefs. Therefore, we believe the regulation appropriately balances the need to access information to determine compliance with the desire of covered entities to avoid opening every record in their possession to the government.

Provision of Technical Assistance

Comment: A number of commenters inquired as to how a covered entity can request technical assistance from the Secretary to come into compliance. A number of commenters suggested that the Secretary provide interpretive guidance to assist with compliance. Others recommended that the Secretary have a contact person or privacy official, available by telephone or email, to provide guidance on the appropriateness of a disclosure or a denial of access. One commenter suggested that there be a formal process for a covered entity to submit compliance activities to the Secretary for prior approval and clarification. This commenter suggested that clarifications be published on a contemporaneous basis in the **Federal Register** to help correct any ambiguities and confusion in implementation. It was also suggested that the Secretary undertake an assessment of ''best practices'' of covered entities and document and promote the findings to serve as a convenient ''road map'' for other covered entities. Another commenter suggested that we work with providers to create implementation guidelines modeled after the interpretative

guidelines that HCFA creates for surveyors on the conditions of participation for Medicare and Medicaid contractors.

Response: While we have not in the final rule committed the Secretary to any specific model of providing guidance or assistance, we do state our intent, subject to budget and staffing constraints, to develop a technical assistance program that will include the provision of written material when appropriate to assist covered entities in achieving compliance. We will consider other models including HCFA's Medicare and Medicaid interpretative guidelines. Further information regarding the Secretary's technical assistance program may be provided in the **Federal Register** and on the HHS Office for Civil Rights (OCR) Web Site. While OCR plans to have fully trained staff available to respond to questions, its ability to provide individualized advice in regard to such matters as the appropriateness of a particular disclosure or the sufficiency of compliance activities will be based on staff resources and demands. The idea of looking at ''best practices'' and sharing information with all covered entities is a good one and we will explore how best to do this. We note that a covered entity is not excused from compliance with the regulation because of any failure to receive technical assistance or guidance.

Basis for Violation Findings and Enforcement

Comment: A number of commenters asked that covered entities not be liable for violations of the rule if they have acted in good faith. One commenter indicated that enforcement actions should not be pursued against covered entities that make legitimate business decisions about how to comply with the privacy standards.

Response: The commenters seemed to argue that even if a covered entity does not comply with a requirement of the rule, the covered entity should not be liable if there was an honest and sincere intention or attempt to fulfill its obligations. The final rule, however, does not take this approach but instead draws careful distinctions between what a covered entity must do unconditionally, and what a covered entity must make certain reasonable efforts to do. In addition, the final rule is clear as to the specific provisions where ''good faith'' is a consideration. For example, a covered entity is permitted to use and disclose protected health information without authorization based on criteria that includes a good faith belief that such use or disclosure is necessary to avert an imminent threat to health or safety (§ 164.512(j)(1)(i)). Therefore, covered entities need to pay careful attention to the specific language in each requirement. However, we note that many of these provisions can be implemented in a variety of ways; e.g, covered entities can exercise business judgement regarding how to conduct staff training.

As to enforcement, a covered entity will not necessarily suffer a penalty solely because an act or omission violates the rule. As we discuss elsewhere, the Department will exercise discretion to consider not only the harm done, but the willingness of the covered entity to achieve voluntary compliance. Further, the Administrative Simplification provisions of HIPAA provide that whether a violation was known or not is relevant in determining whether civil or criminal penalties apply. In addition, if a civil penalty applies, HIPAA allows the Secretary, where the failure to comply was due to reasonable cause and not to willful neglect, to delay the imposition of the penalty to allow the covered entity to comply. The Department will develop and release for public comment an enforcement regulation applicable to all the administrative simplification regulations that will address these issues.

Comment: One commenter asked whether hospitals will be vicariously liable for the violations of their employees and expressed concern that hospitals and other providers will be the ones paying large fines.

Response: The enforcement regulation will address this issue. However, we note that section 1128A(1) of the Social Security Act, which applies to the imposition of civil monetary penalties under HIPAA, provides that a principal is liable for penalties for the actions of its agent acting within the scope of the agency. Therefore, a covered entity will generally be responsible for the actions of its employees such as where the employee discloses protected health information in violation of the regulation.

Comment: A commenter expressed the concern that if a covered entity acquires a non-compliant health plan, it would be liable for financial penalties. This commenter suggested that, at a minimum, the covered entity be given a grace period of at least a year, but not less than six months to bring any acquisition up to standard. The commenter stated that the Secretary should encourage, not discourage, compliant companies to acquire non-compliant ones. Another commenter expressed a general concern about resolution of enforcement if an entity faced with a HIPAA complaint acquires or merges with an entity not covered by HIPAA.

Response: As discussed above, the Secretary will encourage voluntary efforts to cure violations of the rule, and will consider that fact in determining whether to bring a compliance action. We do not agree, however, that we should limit our authority to pursue violations of the rule if the situation warrants it.

Comment: One commenter was concerned about the ''undue risk'' of liability on originators of information, stemming from the fact that ''the number of covered entities is limited and they are unable to restrict how a recipient of information may use or re-disclose information * * *''

Response: Under this rule, we do not hold covered entities responsible for the actions of recipients of protected health information, unless the recipient is a business associate of the covered entity. We agree that it is not fair to hold covered entities responsible for the actions of persons with whom they have no on-going relationship, but believe it is fair to expect covered entities to hold their business associates to appropriate standards of behavior with respect to health information.

Other Compliance and Enforcement Comments

Comment: A number of comments raised questions regarding the Secretary's priorities for enforcement. A few commenters stated that they supported deferring enforcement until there is experience using the proposed standards. One organization asked that we clarify that the regulation does not replace or otherwise modify the self-regulatory/consumer empowerment approach to consumer privacy in the online environment.

Response: We have not made any decisions regarding enforcement priorities. It appears that some commenters believe that no enforcement action will be taken against a given covered entity until that entity has had some time to comply. Covered entities have two years to come into compliance with the regulation (three years in the case of small health plans). Some covered entities will have had experience using the standards prior to the compliance date. We do not agree that we should defer enforcement where violations of the rule occur. It would be wrong for covered entities to believe that enforcement action is based on their not having much experience in

using a particular standard or meeting another requirement.

We support a self-regulation approach in that we recognize that most compliance will be achieved by the voluntary activities of covered entities rather than by our enforcement activities. Our emphasis will be on education, technical assistance, and voluntary compliance and not on finding violations and imposing penalties. We also support a consumer empowerment approach. A knowledgeable consumer is key to the effectiveness of this rule. A consumer familiar with the requirements of this rule will be equipped to make choices regarding which covered entity will best serve their privacy interests and will know their rights under the rule and how they can seek redress for violations of this rule. Privacy-minded consumers will seek to protect the privacy rights of others by bringing concerns to the attention of covered entities, the public, and the Secretary. However, we do not agree that we should defer enforcement where violations of the rule occur.

Comment: One commenter expressed concern that by filing a complaint an individual would be required to reveal sensitive information to the public. Another commenter suggested that complaints regarding noncompliance in regard to psychotherapy notes should be made to a panel of mental health professionals designated by the Secretary. This commenter also proposed that all patient information be maintained as privileged, not be revealed to the public, and be kept under seal after the case is reviewed and closed.

Response: We appreciate this concern and will seek to ensure that individually identifiable health information and other personal information contained in complaints will not be available to the public. The privacy regulation provides, at § 160.310(c)(3), that protected health information obtained by the Secretary in connection with an investigation or compliance review will not be disclosed except if necessary for ascertaining or enforcing compliance with the regulation or if required by law. In addition, this Department generally seeks to protect the privacy of individuals to the fullest extent possible, while permitting the exchange of records required to fulfill its administrative and program responsibilities. The Freedom of Information Act, 5 U.S.C. 552, and the HHS implementing regulation, 45 CFR part 5, provide substantial protection for records about individuals where disclosure would constitute an unwarranted invasion of their personal privacy. In implementing the privacy regulation, OCR plans to continue its current practice of protecting its complaint files from disclosure. OCR treats these files as investigatory records compiled for law enforcement purposes. Moreover, OCR maintains that disclosing protected health information in these files generally constitutes an unwarranted invasion of personal privacy.

It is not clear in regarding the use of mental health professionals, whether the commenter believes that such professionals should be involved because they would be best able to keep psychotherapy notes confidential or because such professionals can best understand the meaning or relevance of such notes. OCR anticipates that it will not have to obtain a copy or review psychotherapy notes in investigating most complaints regarding noncompliance in regard to such notes. There may be some cases where a review of the notes may be needed such as where we need to identify that the information a covered entity disclosed was in fact psychotherapy notes. If we need to obtain a copy of psychotherapy notes, we will keep these notes confidential and secure. OCR investigative staff will be trained to ensure that they fully respect the confidentiality of personal information. In addition, while the specific contents of these notes is generally not relevant to violations under this rule, if such notes are relevant, we will secure the expertise of mental health professionals if needed in reviewing psychotherapy notes.

Comment: A member of Congress and a number of privacy and consumer groups expressed concern with whether OCR has adequate funding to carry out the major responsibility of enforcing the complaint process established by this rule. The Senator stated that ''[d]ue to the limited enforcement ability allowed for in this rule by HIPAA, it is essential that OCR have the capacity to enforce the regulations. Now is the time for OCR to begin building the necessary infrastructure to enforce the regulation effectively.''

Response: We agree and are committed to an effective enforcement program. We are working with Congress to ensure that the Secretary has the necessary funds to secure voluntary compliance through education and technical assistance, to investigate complaints and conduct compliance reviews, to provide states with exception determinations, and to use civil and criminal penalties when necessary. We will continue to work with Congress and within the new Administration in this regard.

Coordination With Reviewing Authorities

Comment: A number of commenters referenced other entities that already consider the privacy of health information. One commenter indicated opposition to the delegation of inspections to third party organizations, such as the Joint Commission on the Accreditation of Healthcare Organizations (JCAHO). A few commenters indicated that state agencies are already authorized to investigate violations of state privacy standards and that we should rely on those agencies to investigate alleged violations of the privacy rules or delegate its complaint process to states that wish to carry out this responsibility or to those states that have a complaint process in place. Another commenter argued that individuals should be required to exhaust any state processes before filing a complaint with the Secretary. Others referenced the fact that state medical licensing boards investigate complaints against physicians for violating patient confidentiality. One group asked that the federal government streamline all of these activities so physicians can have a single entity to whom they must be responsive. Another group suggested that OMB should be given responsibility for ensuring that FEHB Plans operate in compliance with the privacy standards and for enforcement.

A few commenters stated that the regulation might be used as a basis for violation findings and subsequent penalties under other Department authorities, such as under Medicare's Conditions of Participation related to patient privacy and right to confidentiality of medical records. One commenter wanted some assurance that this regulation will not be used as grounds for sanctions under Medicare. Another commenter indicated support for making compliance with the privacy regulation a Condition of Participation under Medicare.

Response: HIPAA does not give the Secretary the authority to delegate her responsibilities to other private or public agencies such as JCAHO or state agencies. However, we plan to explore ways that we may benefit from current activities that also serve to protect the privacy of individually identifiable health information. For example, if we conduct an investigation or review of a covered entity, that entity may want to share information regarding findings of other bodies that conducted similar reviews. We would welcome such

information. In developing its enforcement program, we may explore ways it can coordinate with other regulatory or oversight bodies so that we can efficiently and effectively pursue our joint interests in protecting privacy.

We do not accept the suggestion that individuals be required to exhaust their remedies under state law before filing a complaint with the Secretary. Our rationale is similar to that discussed above in regard to the suggestion that covered entities be required to exhaust a covered entity's internal complaint process before filing a complaint with the Secretary. Congress provided for federal privacy protection and we want to allow individuals the right to this protection without barriers or delay. Covered entities may in their privacy notice inform individuals of any rights they have under state law including any right to file privacy complaints. We do not have the authority to interfere with state processes and HIPAA explicitly provides that we cannot preempt state laws that provide greater privacy protection.

We have not yet addressed the issue as to whether this regulation might be used as a basis for violation findings or penalties under other Department authorities. We note that Medicare conditions of participation require participating providers to have procedures for ensuring the confidentiality of patient records, as well as afford patients with the right to the confidentiality of their clinical records.

Penalties

Comment: Many commenters considered the statutory penalties insufficient to protect privacy, stating that the civil penalties are too weak to have the impact needed to reduce the risk of inappropriate disclosure. Some commenters took the opposing view and stated that large fines and prison sentences for violations would discourage physicians from transmitting any sort of health care information to any other agency, regardless of the medical necessity. Another comment expressed the concern that doctors will be at risk of going to jail for protecting the privacy of individuals (by not disclosing information the government believes should be released).

Response: The enforcement regulation will address the application of the civil monetary and criminal penalties under HIPAA. The regulation will be published in the **Federal Register** as a proposed regulation and the public will have an opportunity to comment. We do not believe that our rule, and the penalties available under it, will discourage physicians and other providers from using or disclosing necessary information. We believe that the rule permits physicians to make the disclosures that they need to make under the health care system without exposing themselves to jeopardy under the rule. We believe that the penalties under the statute are woefully inadequate. We support legislation that would increase the amount of these penalties.

Comment: A number of commenters stated that the regulations should permit individuals to sue for damages caused by breaches of privacy under these regulations. Some of these commenters specified that damages, equitable relief, attorneys fees, and punitive damages should be available. Conversely, one comment stated that strong penalties are necessary and would preclude the need for a private right of action. Another commenter stated that he does not believe that the statute intended to give individuals the equivalent of a right to sue, which results from making individuals third party beneficiaries to contracts between business partners.

Response: We do not have the authority to provide a private right of action by regulation. As discussed below, the final rule deletes the third party beneficiary provision that was in the proposed rule.

However, we believe that, in addition to strong civil monetary penalties, federal law should allow any individual whose rights have been violated to bring an action for actual damages and equitable relief. The Secretary's Recommendations, which were submitted to Congress on September 11, 1997, called for a private right of action to permit individuals to enforce their privacy rights.

Comment: One comment stated that, in calculating civil monetary penalties, the criteria should include aggravating or mitigating circumstances and whether the violation is a minor or first time violation. Several comments stated that penalties should be tiered so that those that commit the most egregious violations face stricter civil monetary penalties.

Response: As mentioned above, issues regarding civil fines and criminal penalties will be addressed in the enforcement regulation.

Comment: One comment stated that the regulation should clarify whether a single disclosure that involved the health information of multiple parties would constitute a single or multiple infractions, for the purpose of calculating the penalty amount.

Response: The enforcement regulation will address the calculation of penalties. However, we note that section 1176 subjects persons to civil monetary penalties of not more than $100 for each violation of a requirement or prohibition and not more than $25,000 in a calendar year for all violations of an identical requirement or prohibition. For example, if a covered entity fails to permit amendment of protected health information for 10 patients in one calendar year, the entity may be fined up to $1000 ($100 times 10 violations equals $1000).

Part 164—Subpart A—General Requirements

Part 164—Subpart B–D—Reserved

Part 164—Subpart E—Privacy

Section 164.500—Applicability

Covered Entities

The response to comments on covered entities is included in the response to comments on the definition of ''covered entity'' in the preamble discussion of § 160.103.

Covered Information

The response to comments on covered information is included in the response to comments on the definition of ''protected health information'' in the preamble discussion of § 164.501.

Section 164.501—Definitions

Designated record set

Comment: Many commenters generally supported our proposed definition of designated record set. Commenters suggested different methods for narrowing the information accessible to individuals, such as excluding information obtained without face-to-face interaction (e.g., phone consultations). Other commenters recommended broadening the information accessible to individuals, such as allowing access to ''the entire medical record,'' not just a designated record set. Some commenters advocated for access to all information about individuals. A few commenters generally supported the provision but recommended that consultation and interpretative assistance be provided when the disclosure may cause harm or misunderstanding.

Response: We believe individuals should have a right to access any protected health information that may be used to make decisions about them and modify the final rule to accomplish this result. This approach facilitates an open and cooperative relationship between individuals and covered health care providers and health plans and allows individuals fair opportunities to know what health information may be

used to make decisions about them. We list certain records that are always part of the designated record set. For covered providers these are the medical record and billing record. For health plans these are the enrollment, payment, claims adjudication, and case or medical management records. The purpose of these specified records is management of the accounts and health care of individuals. In addition, we include in the designated record set to which individuals have access any record used, in whole or in part, by or for the covered entity to make decisions about individuals. Only protected health information that is in a designated record set is covered. Therefore, if a covered provider has a phone conversation, information obtained during that conversation is subject to access only to the extent that it is recorded in the designated record set.

We do not require a covered entity to provide access to all individually identifiable health information, because the benefits of access to information not used to make decisions about individuals is limited and is outweighed by the burdens on covered entities of locating, retrieving, and providing access to such information. Such information may be found in many types of records that include significant information not relevant to the individual as well as information about other persons. For example, a hospital's peer review files that include protected health information about many patients but are used only to improve patient care at the hospital, and not to make decisions about individuals, are not part of that hospital's designated record sets.

We encourage but do not require covered entities to provide interpretive assistance to individuals accessing their information, because such a requirement could impose administrative burdens that outweigh the benefits likely to accrue.

The importance to individuals of having the right to inspect and copy information about them is supported by a variety of industry groups and is recognized in current state and federal law. The July 1977 Report of the Privacy Protection Study Commission recommended that individuals have access to medical records and medical record information.[2] The Privacy Act (5 U.S.C. 552a) requires government agencies to permit individuals to review records and have a copy made in a form comprehensible to the individual. In its report ''Best Principles for Health Privacy,'' the Health Privacy Working Group recommended that individuals should have the right to access information about them.[3] The National Association of Insurance Commissioners' Health Information Privacy Model Act establishes the right of an individual to examine or receive a copy of protected health information in the possession of the carrier or a person acting on behalf of the carrier.

Many states also establish a right for individuals to access health information about them. For example, Alaska law (AK Code 18.23.005) entitles patients ''to inspect and copy any records developed or maintained by a health care provider or other person pertaining to the health care rendered to the patient.'' Hawaii law (HRS section 323C–11) requires health care providers and health plans, among others, to permit individuals to inspect and copy protected health information about them. Many other states have similar provisions.

Industry and standard-setting organizations also have developed policies to enable individual access to health information. The National Committee for Quality Assurance and the Joint Commission on Accreditation of Healthcare Organizations issued recommendations stating, ''Patients' confidence in the protection of their information requires that they have the means to know what is contained in their records. The opportunity for patients to review their records will enable them to correct any errors and may provide them with a better understanding of their health status and treatment.'' [4] Standards of the American Society for Testing and Materials state, ''The patient or his or her designated personal representative has access rights to the data and information in his or her health record and other health information databases except as restricted by law. An individual should be able to inspect or see his or her health information or request a copy of all or part of the health information, or both.'' [5] We build on this well-established principle in this final rule.

Comment: Several commenters advocated for access to not only information that has already been used to make decisions, but also information that may be used to make decisions. Other commenters believed accessible information should be more limited; for example, some commenters argued that accessible information should be restricted to only information used to make health care decisions.

Response: We agree that it is desirable that individuals have access to information reasonably likely to be used to make decisions about them. On the other hand, it is desirable that the category of records covered be readily ascertainable by the covered entity. We therefore define ''designated record set'' to include certain categories of records (a provider's medical record and billing record, the enrollment records, and certain other records maintained by a health plan) that are normally used, and are reasonably likely to be used, to make decisions about individuals. We also add a category of other records that are, in fact, used, in whole or in part, to make decisions about individuals. This category includes records that are used to make decisions about any individuals, whether or not the records have been used to make a decision about the particular individual requesting access.

We disagree that accessible information should be restricted to information used to make health care decisions, because other decisions by covered entities can also affect individuals' interests. For example, covered entities make financial decisions about individuals, such as whether an individual's deductible has been met. Because such decisions can significantly affect individuals' interests, we believe they should have access to any protected health information included in such records.

Comment: Some commenters believed the rule should use the term ''retrievable'' instead of ''retrieved'' to describe information accessible to individuals. Other commenters suggested that the rule follow the Privacy Act's principle of allowing access only when entities retrieve records by individual identifiers. Some commenters requested clarification that covered entities are not required to maintain information by name or other patient identifier.

Response: We have modified the proposed definition of the designated record set to focus on how information is used, not how it is retrieved. Information may be retrieved or retrievable by name, but if it is never used to make decisions about any

[2] Privacy Protection Study Commission, ''Personal Privacy in an Information Society,'' July 1977, p. 298–299.

[3] Health Privacy Working Group, ''Best Principles for Health Privacy,'' Health Privacy Project, Institute for Health Care Research and Policy, Georgetown University, July 1999.

[4] National Committee on Quality Assurance and the Joint Commission on Accreditation of Healthcare Organizations, ''Protecting Personal Health Information: A Framework for Meeting the Challenges in a Managed Care Environment,'' 1998, p. 25.

[5] ASTM, ''Standard Guide for Confidentiality, Privacy, Access and Data Security, Principles for Health Information Including Computer-Based Patient Records,'' E 1869–97, § 11.1.1.

individuals, the burdens of requiring a covered entity to find it and to redact information about other individuals outweigh any benefits to the individual of having access to the information. When the information might be used to affect the individual's interests, however, that balance changes and the benefits outweigh the burdens. We confirm that this regulation does not require covered entities to maintain any particular record set by name or identifier.

Comment: A few commenters recommended denial of access for information relating to investigations of claims, fraud, and misrepresentations. Many commenters suggested that sensitive, proprietary, and legal documents that are ''typical state law privileges'' be excluded from the right to access. Specific suggestions for exclusion, either from the right of access or from the definition of designated record set, include quality assurance activities, information related to medical appeals, peer review and credentialing, attorney-client information, and compliance committee activities. Some commenters suggested excluding information already supplied to individuals on previous requests and information related to health care operations. However, some commenters felt that such information was already excluded from the definition of designated record set. Other commenters requested clarification that this provision will not prevent patients from getting information related to medical malpractice.

Response: We do not agree that records in these categories are never used to affect the interests of individuals. For example, while protected health information used for peer review and quality assurance activities typically would not be used to make decisions about individuals, and, thus, typically would not be part of a designated record set, we cannot say that this is true in all cases. We design this provision to be sufficiently flexible to work with the varying practices of covered entities.

The rule addresses several of these comments by excepting from the access provisions (§ 164.524) information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding. Similarly, nothing in this rule requires a covered entity to divulge information covered by physician-patient or similar privilege. Under the access provisions, a covered entity may redact information in a record about other persons or information obtained under a promise of confidentiality, prior to releasing the information to the individual. We clarify that nothing in this provision would prevent access to information needed to prosecute or defend a medical malpractice action; the rules of the relevant court determine such access.

We found no persuasive evidence to support excluding information already supplied to individuals on previous requests. The burdens of tracking requests and the information provided pursuant to requests outweigh the burdens of providing the access requested. A covered entity may, however, discuss the scope of the request for access with the individual to facilitate the timely provision of access. For example, if the individual agrees, the covered entity could supply only the information created or received since the date access was last granted.

Disclosure

Comment: A number of commenters asked that the definition of ''disclosure'' be modified so that it is clear that it does not include the release, transfer, provision of access to, or divulging in any other manner of protected health information to the individual who is the subject of that information. It was suggested that we revise the definition in this way to clarify that a health care provider may release protected health information to the subject of the information without first requiring that the patient complete an authorization form.

Response: We agree with the commenters' concern, but accomplish this result through a different provision in the regulation. In § 164.502 of this final rule, we specify that disclosures of protected health information to the individual are not subject to the limitations on disclosure of protected health information otherwise imposed by this rule.

Comment: A number of commenters stated that the regulation should not apply to disclosures occurring within or among different subsidiaries or components of the same entity. One commenter interpreted ''disclosure'' to mean outside the agency or, in the case of a state Department of Health, outside sister agencies and offices that directly assist the Secretary in performing Medicaid functions and are listed in the state plan as entitled to receive Medicaid data.

Response: We agree that there are circumstances under which related organizations may be treated as a single covered entity for purposes of protecting the privacy of health information, and modify the rule to accommodate such circumstances. In § 164.504 of the final rule, we specify the conditions under which affiliated companies may combine into a single covered entity and similarly describe which components of a larger organization must comply with the requirements of this rule. For example, transfers of information within the designated component or affiliated entity are uses while transfers of information outside the designated component or affiliated entity are disclosures. See the discussion of § 164.504 for further information and rationale. It is not clear from these comments whether the particular organizational arrangements described could constitute a single covered entity.

Comment: A commenter noted that the definition of ''disclosure'' should reflect that health plan correspondence containing protected health information, such as Explanation of Benefits (EOBs), is frequently sent to the policyholder. Therefore, it was suggested that the words ''provision of access to'' be deleted from the definition and that a ''disclosure'' be clarified to include the conveyance of protected health information to a third party.

Response: The definition is, on its face, broad enough to cover the transfers of information described and so is not changed. We agree that health plans must be able to send EOBs to policyholders. Sending EOB correspondence to a policyholder by a covered entity is a disclosure for purposes of this rule, but it is a disclosure for purposes of payment. Therefore, subject to the provisions of § 164.522(b) regarding Confidential Communications, it is permitted even if it discloses to the policyholder protected health information about another individual (see below).

Health care operations

Comment: Several commenters stated that the list of activities within the definition of health care operations was too broad and should be narrowed. They asserted that the definition should be limited to exclude activities that have little or no connection to the care of a particular patient or to only include emergency treatment situations or situations constituting a clear and present danger to oneself or others.

Response: We disagree. We believe that narrowing the definition in the manner requested will place serious burdens on covered entities and impair their ability to conduct legitimate business and management functions.

Comment: Many commenters, including physician groups, consumer groups, and privacy advocates, argued that we should limit the information that can be used for health care operations to de-identified data. They

argued that if an activity could be done with de-identified data, it should not be incorporated in the definition of health care operations.

Response: We disagree. We believe that many activities necessary for the business and administrative operations of health plans and health care providers are not possible with de-identified information or are possible only under unduly burdensome circumstances. For example, identified information may be used or disclosed during an audit of claims, for a plan to contact a provider about alternative treatments for specific patients, and in reviewing the competence of health care professionals. Further, not all covered entities have the same ability to de-identify protected health information. Covered entities with highly automated information systems will be able to use de-identified data for many purposes. Other covered entities maintain most of their records on paper, so a requirement to de-identify information would place too great a burden on the legitimate and routine business functions included in the definition of health care operations. Small business, which are most likely to have largely paper records, would find such a blanket requirement particularly burdensome.

Protected health information that is de-identified pursuant to § 164.514(a) is not subject to this rule. We hope this provides covered entities capable of de-identifying information with the incentive to do so.

Comment: Some commenters requested that we permit the use of demographic data (geographic, location, age, gender, and race) separate from all other data for health care operations. They argued that demographic data was needed to establish provider networks and monitor providers to ensure that the needs of ethnic and minority populations were being addressed.

Response: The use of demographic data for the stated purposes is within the definition of health care operations; a special rule is not necessary.

Comment: Some commenters pointed out that the definition of health care operations is similar to, and at times overlaps with, the definition of research. In addition, a number of commenters questioned whether or not research conducted by the covered entity or its business partner must only be applicable to and used within the covered entity to be considered health care operations. Others questioned whether such studies or research performed internal to a covered entity are ''health care operations'' even if generalizable results may be produced.

Response: We agree that some health care operations have many of the characteristics of research studies and in the NPRM asked for comments on how to make this distinction. While a clear answer was not suggested in any of the comments, the comments generally together with our fact finding lead to the provisions in the final rule. The distinction between health care operations and research rests on whether the primary purpose of the study is to produce ''generalizable knowledge.'' We have modified the definition of health care operations to include ''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.*'' If the primary purpose of the activity is to produce generalizable knowledge, the activity fits within this rule's definition of ''research'' and the covered entity must comply with §§ 164.508 or 164.512, including obtaining an authorization or the approval of an institutional review board or privacy board. If not and the activity otherwise meets the definition of health care operations, the activity is not research and may be conducted under the health care operations provisions of this rule.

In some instances, the primary purpose of the activity may change as preliminary results are analyzed. An activity that was initiated as an internal outcomes evaluation may produce information that the covered entity wants to generalize. If the purpose of a study changes and the covered entity does intend to generalize the results, the covered entity should document the change in status of the activity to establish that they did not violate the requirements of this rule. (See definition of ''research,'' below, for further information on the distinction between ''research'' and ''health care operations.'')

We note that the difficulty in determining when an activity is for the internal operations of an entity and when it is a research activity is a long-standing issue in the industry. The variation among commenters' views is one of many indications that, today, there is not consensus on how to draw this line. We do not resolve the larger issue here, but instead provide requirements specific to the information covered by this rule.

Comment: Several commenters asked that disease management and disability management activities be explicitly included in the definition of health care operations. Many health plans asserted that they would not be able to provide disease management, wellness, and health promotion activities if the activity were solely captured in the rule's definition of ''treatment.'' They also expressed concern that ''treatment'' usually applies to an individual, not to a population, as is the practice for disease management.

Response: We were unable to find generally accepted definitions of the terms ''disease management'' and ''disability management.'' Rather than rely on this label, we include many of the functions often included in discussions of disease management in this definition or in the definition of treatment, and modify both definitions to address the commenters' concerns. For example, we have revised the definition of health care operations to include population-based activities related to improving health or reducing health care costs. This topic is discussed further in the comment responses regarding the definition of ''treatment,'' below.

Comment: Several commenters urged that the definition of health care operations be illustrative and flexible, rather than structured in the form of a list as in the proposed rule. They believed it would be impossible to identify all the activities that constitute health care operations. Commenters representing health plans were concerned that the ''static'' nature of the definition would stifle innovation and could not reflect the new functions that health plans may develop in the future that benefit consumers, improve quality, and reduce costs. Other commenters, expressed support for the approach taken in the proposed rule, but felt the list was too broad.

Response: In the final rule, we revise the proposed definition of health care operations to broaden the list of activities included, but we do not agree with the comments asking for an illustrative definition rather than an inclusive list. Instead, we describe the activities that constitute health care operations in broad terms and categories, such as ''quality assessment'' and ''business planning and development.'' We believe the use of broadly stated categories will allow industry innovation, but without the privacy risks entailed in an illustrative approach.

Comment: Several commenters noted that utilization review and internal quality review should be included in the definition. They pointed out that both of these activities were discussed in the preamble to the proposed rule but were not incorporated into the regulation text.

Response: We agree and have modified the regulation text to incorporate quality assessment and improvement activities, including the development of clinical guidelines and protocol development.

Comment: Several commenters stated that the proposal did not provide sufficient guidance regarding compiling and analyzing information in anticipation of or for use in legal proceedings. In particular, they raised concerns about the lack of specificity as to when ''anticipation'' would be triggered.

Response: We agree that this provision was confusing and have replaced it with a broader reference to conducting or arranging for legal services generally.

Comment: Hospital representatives pointed out the pressure on health care facilities to improve cost efficiencies, make cost-effectiveness studies, and benchmark essential health care operations. They emphasized that such activities often use identifiable patient information, although the products of the analyses usually do not contain identifiable health information. Commenters representing state hospital associations pointed out that they routinely receive protected health information from hospitals for analyses that are used by member hospitals for such things as quality of care benchmark comparisons, market share analysis, determining physician utilization of hospital resources, and charge comparisons.

Response: We have expanded the definition of health care operations to include use and disclosure of protected health information for the important functions noted by these commenters. We also allow a covered entity to engage a business associate to provide data aggregation services. See § 164.504(e).

Comment: Several commenters argued that many activities that are integral to the day-to-day operations of a health plan have not been included in the definition. Examples provided by the commenters include: issuing plan identification cards, customer service, computer maintenance, storage and back-up of radiologic images, and the installation and servicing of medical equipment or computer systems.

Response: We agree with the commenters that there are activities not directly part of treatment or payment that are more closely associated with the administrative or clerical functions of the plan or provider that need to be included in the definition. To include such activities in the definition of health care operations, we eliminate the requirement that health care operations be directly related to treatment and payment, and we add to this definition the new categories of business management (including general administrative activities) and business planning activities.

Comment: One commenter asked for clarification on whether cost-related analyses could also be done by providers as well as health plans.

Response: Health care operations, including business management functions, are not limited to health plans. Any covered entity can perform health care operations.

Comment: One commenter stated that the proposed rule did not address what happens to records when a covered entity is sold or merged with another entity.

Response: We agree and add to the definition of health care operations disclosures of protected health information for due diligence to a covered entity that is a potential successor in interest. This provision includes disclosures pursuant to the sale of a covered entity's business as a going concern, mergers, acquisitions, consolidations, and other similar types of corporate restructuring between covered entities, including a division of a covered entity, and to an entity that is not a covered entity but will become a covered entity if the reorganization or sale is completed. Other types of sales of assets, or disclosures to organizations that are not and would not become covered entities, are not included in the definition of health care operations and could only occur if the covered entity obtained valid authorization for such disclosure in accordance with § 164.508 or if the disclosure is otherwise permitted under this rule.

Once a covered entity is sold or merged with another covered entity, the successor in interest becomes responsible for complying with this regulation with respect to the transferred information.

Comment: Several commenters expressed concern that the definition of health care operations failed to include the use of protected health information for the underwriting of new health care policies and took issue with the exclusion of uses and disclosures of protected health information of prospective enrollees. They expressed the concern that limiting health care operations to the underwriting and rating of existing members places a health plan in the position of not being able to evaluate prudently and underwrite a consumer's health care risk.

Response: We agree that covered entities should be able to use the protected health information of prospective enrollees to underwrite and rate new business and change the definition of health care operations accordingly. The definition of health care operations below includes underwriting, premium rating, and other activities related to the creation of a contract of health insurance.

Comment: Several commenters stated that group health plans needed to be able to use and disclose protected health information for purposes of soliciting a contract with a new carrier and rate setting.

Response: We agree and add ''activities relating to the * * * replacement of a contract of insurance'' to cover such disclosures. See § 164.504 for the rules for plan sponsors of group health plans to obtain such information.

Comment: Commenters from the business community supported our recognition of the importance of financial risk transfer mechanisms in the health care marketplace by including ''reinsurance'' in the definition of health care operations. However, they stated that the term ''reinsurance'' alone was not adequate to capture ''stop-loss insurance'' (also referred to as excess of loss insurance), another type of risk transfer insurance.

Response: We agree with the commenters that stop-loss and excess of loss insurance are functionally equivalent to reinsurance and add these to the definition of health care operations.

Comment: Commenters from the employer community explained that there is a trend among employers to contract with a single insurer for all their insurance needs (health, disability, workers' compensation). They stated that in these integrated systems, employee health information is shared among the various programs in the system. The commenters believed the existing definition poses obstacles for those employers utilizing an integrated health system because of the need to obtain authorizations before being permitted to use protected health information from the health plan to administer or audit their disability or workers' compensation plan.

Other commenters representing employers stated that some employers wanted to combine health information from different insurers and health plans providing employee benefits to their workforces, including its group health plan, workers' compensation insurers, and disability insurers, so that they could have more information in order to better manage the occurrences of disability and illness among their workforces. They expressed concern

that the proposed rule would not permit such sharing of information.

Response: While we agree that integrating health information from different benefit programs may produce efficiencies as well as benefits for individuals, the integration also raises significant privacy concerns, particularly if there are no safeguards on uses and disclosures from the integrated data. Under HIPAA, we do not have jurisdiction over many types of insurers that use health information, such as workers' compensation insurers or insurers providing disability income benefits, and we cannot address the extent to which they provide individually identifiable health information to a health plan, nor do we prohibit a health plan from receiving such information. Once a health plan receives identifiable health information, however, the information becomes protected and may only be used and disclosed as otherwise permitted by this rule.

We clarify, however, that a covered entity may provide data and statistical analyses for its customers as a health care operation, provided that it does not disclose protected health information in a way that would otherwise violate this rule. A group health plan or health insurance issuer or HMO, or their business associate on their behalf, may perform such analyses for an employer customer and provide the results in de-identified form to the customer, using integrated data received from other insurers, as long as protected health information is not disclosed in violation of this rule. See the definition of ''health care operations,'' § 164.501. If the employer sponsors more than one group health plan, or if its group health plan provides coverage through more than one health insurance issuer or HMO, the different covered entities may be an organized health care arrangement and be able to jointly participate in such an analysis as part of the health care operations of such organized health care arrangement. See the definitions of ''health care operations'' and ''organized health care arrangement,'' § 164.501. We further clarify that a plan sponsor providing plan administration to a group health plan may participate in such an analysis, provided that the requirements of § 164.504(f) and other parts of this rule are met.

The results described above are the same whether the health information that is being combined is from separate insurers or from one entity that has a health component and also provides excepted benefits. See the discussion relating to health care components, § 164.504.

We note that under the arrangements described above, the final rule provides substantial flexibility to covered entities to provide general data and statistical analyses, resulting in the disclosure of de-identified information, to employers and other customers. An employer also may receive protected health information from a covered entity for any purpose, including those described in comment above, with the authorization of the individual. See § 164.508.

Comment: A number of commenters asserted that the proposed definition appeared to limit training and educational activities to that of health care professionals, students, and trainees. They asked that we expand the definition to include other education-related activities, such as continuing education for providers and training of non-health care professionals as needed for supporting treatment or payment.

Response: We agree with the commenters that the definition of health care operations was unnecessarily limiting with respect to educational activities and expand the definition of health care operations to include ''conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers.'' We clarify that medical rounds are considered treatment, not health care operations.

Comment: A few commenters outlined the need to include the training of non-health care professionals, such as health data analysts, administrators, and computer programmers within the definition of health care operations. It was argued that, in many cases, these professionals perform functions which support treatment and payment and will need access to protected health information in order to carry out their responsibilities.

Response: We agree and expand the definition of health care operations to include training of non-health care professionals.

Comment: One commenter stated that the definition did not explicitly include physician credentialing and peer review.

Response: We have revised the definition to specifically include ''licensing or credentialing activities.'' In addition, peer review activities are captured in the definition as reviewing the competence or qualifications of health care professionals and evaluating practitioner and provider performance.

Health Oversight Agency

Comment: Some commenters sought to have specific organizations defined as health oversight agencies. For example, some commenters asked that the regulation text, rather than the preamble, explicitly list state insurance departments as an example of health oversight agencies. Medical device manufacturers recommended expanding the definition to include government contractors such as coding committees, which provide data to HCFA to help the agency make reimbursement decisions.

One federal agency sought clarification that several of its sub-agencies were oversight agencies; it was concerned about its status in part because the agency fits into more than one of the categories of health oversight agency listed in the proposed rule.

Other commenters recommended expanding the definition of oversight agency to include private-sector accreditation organizations. One commenter recommended stating in the final rule that private companies providing information to insurers and employers are not included in the definition of health oversight agency.

Response: Because the range of health oversight agencies is so broad, we do not include specific examples in the definition. We include many examples in the preamble above and provide further clarity here.

As under the NPRM, state insurance departments are an example of a health oversight agency. A commenter concerned about state trauma registries did not describe the registries' activities or legal charters, so we cannot clarify whether such registries may be health oversight agencies. Government contractors such as coding committees, which provide data to HCFA to support payment processes, are not thereby health oversight agencies under this rule. We clarify that public agencies may fit into more than one category of health oversight agency.

The definition of health oversight agency does not include private-sector accreditation organizations. While their work can promote quality in the health care delivery system, private accreditation organizations are not authorized by law to oversee the health care system or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant. Under the final rule, we consider private accrediting groups to be performing a health care operations function for covered entities. Thus, disclosures to private accrediting organizations are