prohibited under § 164.502(a)(1) from using or disclosing protected health information for the purpose(s) included in the consent. A covered entity that seeks a consent must adhere to the individual's decision.

In § 164.506(a)(5), we specify that a consent obtained by one covered entity is not effective to permit another covered entity to use or disclose protected health information, unless the consent is a joint consent. See § 164.506(f) and the corresponding preamble discussion below regarding joint consents. A consent provides the individual's permission only for the covered entity that obtains the consent to use or disclose protected health information for treatment, payment, and health care operations. A consent under this section does not operate to authorize another covered entity to use or disclose protected health information, except where the other covered entity is operating as a business associate. We note that, where a covered entity is acting as a business associate of another covered entity, the business associate covered entity is acting for or on behalf of the principal covered entity, and its actions for or on behalf of the principal covered entity are authorized by the consent obtained by the principal covered entity. Thus, under this section, a health plan can obtain a consent that permits the health plan and its business associates to use and disclose protected health information that the health plan and its business associates create or receive. That consent cannot, however, permit another covered entity (that is not a business associate) to disclose protected health information to the health plan or to any other person.

If a covered entity wants to obtain the individual's permission for another covered entity to disclose protected health information to it for treatment, payment, or health care operations purposes, it must seek an authorization in accordance with § 164.508(e). For example, when a covered provider asks the individual for written permission to obtain the individual's medical record from another provider for treatment purposes, it must do so with an authorization, not a consent. Since the permission is for disclosure of protected health information by another person, a consent may not be used.

Section 164.506(b)—Consent General Requirements

In the final rule, we permit a covered health care provider to condition the provision of treatment on the receipt of the individual's consent for the covered provider to use and disclose protected health information to carry out treatment, payment, and health care operations. Covered providers may refuse to treat individuals who do not consent to uses and disclosures for these purposes. See § 164.506(b)(1). We note that there are exceptions to the consent requirements for covered health care providers that are required by law to treat individuals. See § 164.506(a)(3), described above.

Similarly, in the final rule, we permit health plans to condition an individual's enrollment in the health plan on the receipt of the individual's consent for the health plan to use and disclose protected health information to carry out treatment, payment, and health care operations, if the consent is sought in conjunction with the enrollment process. If the health plan seeks the individual's consent outside of the enrollment process, the health plan may not condition any services on obtaining such consent.

Under § 164.520, covered entities must produce a notice of privacy practices. A consent may not be combined in a single document with the notice of privacy practices. See § 164.506(b)(3).

Under § 164.506(b)(4), consents for uses and disclosures of protected health information to carry out treatment, payment, and health care operations may be combined in a single document covering all three types of activities and may be combined with other types of legal permission from the individual. For example, a consent to use or disclose protected health information under this rule may be combined with an informed consent to receive treatment, a consent to assign payment of benefits to a provider, or narrowly tailored consents required under state law for the use or disclosure of specific types of protected health information (*e.g.,* state laws requiring specific consent for any sharing of information related to HIV/AIDS).

Within a single consent document, the consent for use and disclosure of protected health information required or permitted under this rule must be visually and organizationally separate from the other consents or authorizations and must be separately signed by the individual and dated.

Where research includes treatment of the individual, a consent under this rule may be combined with the authorization for the use or disclosure of protected health information created for the research, in accordance with § 164.508(f). (This is the only case in which an authorization under § 164.508 of this rule may be combined with a consent under § 164.506 of this rule. See § 164.508(b)(3).) The covered entity that is creating protected health information for the research may elect to combine the consent required under this section with the research-related authorization required under § 164.508(f). For example, a covered health care provider that provides health care to an individual for research purposes and for non-research purposes must obtain a consent under this section for all of the protected health information it maintains. In addition, it must obtain an authorization in accordance with § 164.508(f) which describes how it will use and disclose the protected health information it creates for the research for purposes of treatment, payment, and health care operations. Section 164.506(b)(4) permits the covered entity to satisfy these two requirements with a single document. See § 164.508(f) and the corresponding preamble discussion for a more detailed description of research authorization requirements.

Under § 164.506(b)(5), individuals may revoke a consent in writing at any time, except to the extent that the covered entity has taken action in reliance on the consent. Upon receipt of the written revocation, the covered entity must stop processing the information for use or disclosure, except to the extent that it has taken action in reliance on the consent. A covered health care provider may refuse, under this rule, to continue to treat an individual that revokes his or her consent. A health plan may disenroll an individual that revokes a consent that was sought in conjunction with the individual's enrollment in the health plan.

Covered entities must document and retain any signed consent as required by § 164.530(j).

Section 164.506(c)—Consent Content Requirements

Under § 164.506(c), the consent must be written in plain language. See the preamble discussion regarding notice of privacy practices for a description of plain language requirements. We do not provide a model consent in this rule. We will provide further guidance on drafting consent documents prior to the compliance date.

Under § 164.506(c)(1), the consent must inform the individual that protected health information may be used and disclosed by the covered entity to carry out treatment, payment, or health care operations. The covered entity must determine which of these elements (use and/or disclosure; treatment, payment, and/or health care operations) to include in the consent

document, as appropriate for the covered entity's practices.

For covered health care providers that are required to obtain consent, the requirement applies only to the extent the covered provider uses or discloses protected health information. For example, if all of a covered provider's health care operations are conducted by members of the covered provider's own workforce, the covered provider may choose to obtain consent only for uses, not disclosures, of protected health information to carry out health care operations. If an individual pays out of pocket for all services received from the covered provider and the provider will not disclose any information about the patient to a third party payor, the provider may choose not to obtain the individual's consent to disclose information for payment purposes. In order for a covered provider to be able to use and disclose information for all three purposes, however, all three purposes must be included in the consent.

Under §§ 164.506(c)(2) and (3), the consent must refer the individual to the covered entity's notice for additional information about the uses and disclosures of information described in the consent. The consent must also indicate that the individual has the right to review the notice prior to signing the consent. If the covered entity has reserved the right to change its privacy practices in accordance with § 164.520(b)(1)(v)(C), the consent must indicate that the terms of the notice may change and must describe how the individual may obtain a revised notice. See § 164.520 and the corresponding preamble discussion regarding notice requirements.

Under § 164.506(c)(4), the consent must inform individuals that they have the right to request restrictions on uses and disclosures of protected health information for treatment, payment, and health care operations purposes. It must also state that the covered entity is not required to agree to an individual's request, but that if the covered entity does agree to the request, the restriction is binding on the covered entity. See § 164.522(a) regarding the right to request restrictions.

Under § 164.506(c)(5), the consent must indicate that the individual has the right to revoke the consent in writing, except to the extent that the covered entity has taken action in reliance on the consent.

Under § 164.506(c)(6), the consent must include the individual's signature and the date of signature. Once we adopt the standards for electronic signature, another of the required administrative simplification standards we are required to adopt under HIPAA, an electronic signature that meets those standards will be sufficient under this rule. We do not require any verification of the individual's identity or authentication of the individual's signature. We expect covered health care providers that are required to obtain consent to employ the same level of scrutiny to these signatures as they do to the signature obtained on a document regarding the individual's consent to undergo treatment by the provider.

Section 164.506(d)—Defective Consents

Under § 164.506(d), there is no ''consent'' within the meaning of the rule if the completed document lacks a required element or if the individual has revoked the consent in accordance with § 164.506(b)(5).

Section 164.506(e)—Resolving Conflicting Consents and Authorizations

Situations may arise where a covered entity that has obtained the individual's consent for the covered entity to use or disclose protected health information to carry out treatment, payment, or health care operations is asked to disclose protected health information pursuant to another written legal permission from the individual, such as an authorization, that was obtained by another person. Under § 164.506(e), when the terms of a covered entity's consent conflict with the terms of another written legal permission from the individual to use or disclose protected health information (such as a consent obtained under state law by another covered entity or an authorization), the covered entity must adhere to the more restrictive document. By conflict, we mean that the consent and authorization contain inconsistencies. In implementing this section, we note that the consent under this section references the notice provided to the individual and the individual's right to request restrictions. In determining whether the covered entity's consent conflicts with another written legal permission provided by the individual, the covered entity must consider any limitations on its uses or disclosures resulting from the notice provided to the individual or from restrictions to which it has agreed. For example, a covered nursing home may elect to ask the patient to sign an authorization for the patient's covered primary care physician to forward the patient's medical records to the nursing home. The physician may have previously obtained the individual's consent for disclosure for treatment purposes. If the authorization obtained by the nursing home grants permission for the physician to disclose particular types of information, such as genetic information, but the consent obtained by the physician excludes such information or the physician has agreed to a restriction on that type of information, the physician may not disclose that information. The physician must adhere to the more restrictive written legal permission from the individual.

When a conflict between a consent and another written legal permission from the individual exists, as described above, the covered entity may attempt to resolve the conflict with the individual by either obtaining a new consent from the individual or by having a discussion or otherwise communicating with the individual to determine the individual's preference regarding the use or disclosure. If the individual's preference is communicated orally, the covered entity must document the individual's preference and act in accordance with that preference. In the example described above, the primary care physician could ask the patient to sign a new consent that would permit the disclosure of the genetic information. Alternatively, the physician could ask the patient whether the patient intended for the genetic information to be disclosed to the nursing home. If the patient confirms that he or she intended for the genetic information to be shared, the physician can document that fact (*e.g.,* by making a notation in the medical record) and disclose the information to the nursing home.

We believe covered entities will rarely be faced with conflicts between consents and other written legal permission from the individual for uses and disclosures to carry out treatment, payment, and health care operations. Under § 164.506(a)(5), we specify that a consent only permits the covered entity that obtains the consent to use or disclose protected health information. A consent obtained by one covered entity is not effective to permit another different covered entity to use or disclose protected health information. Conflicting consents obtained by covered entities, therefore, are not possible. We expect authorizations that permit another covered entity to use and disclose protected health information for treatment, payment, and health care operations purposes will rarely be necessary, because we expect covered entities that maintain protected health information to obtain consents that permit them to make anticipated uses and disclosures for these purposes. Nevertheless, covered entities are permitted under § 164.508(e) to obtain

authorization for another covered entity to use or disclose protected health information to carry out treatment, payment, and health care operations. We recognize these authorizations may be useful to demonstrate an individual's intent and relationship to the intended recipient of the information. For example, these authorizations may be useful in situations where a health plan wants to obtain information from one provider in order to determine payment of a claim for services provided by a different provider (e.g., information from a primary care physician that is necessary to determine payment of services provided by a specialist) or where an individual's new physician wants to obtain the individual's medical records from prior physicians. Other persons not covered by this rule may also seek authorizations and state law may require written permission for specific types of information, such as information related to HIV/AIDS or to mental health. Because an individual may sign conflicting documents over time, we clarify that the covered entity maintaining the protected health information to be used or disclosed must adhere to the more restrictive permission the individual has granted, unless the covered entity resolves the conflict with the individual.

Section 164.506(f)—Joint Consents

Covered entities that participate in an organized health care arrangement and that develop a joint notice under § 164.520(d) may develop a joint consent in which the individual consents to the uses and disclosures of protected health information by each of the covered entities in the arrangement to carry out treatment, payment, and/or health care operations. The joint consent must identify with reasonable specificity the covered entities, or class of covered entities, to which the joint consent applies and must otherwise meet the consent requirements. If an individual revokes a joint consent, the covered entity that receives the revocation must inform the other entities covered by the joint consent of the revocation as soon as practicable.

If any one of the covered entities included in the joint consent obtains the individual's consent, as required above, the consent requirement is met for all of the other covered entities to which the consent applies. For example, a covered hospital and the clinical laboratory and emergency departments with which it participates in an organized health care arrangement may produce a joint notice and obtain a joint consent. If the covered hospital obtains the individual's joint consent upon admission, and some time later the individual is readmitted through the associated emergency department, the emergency department's consent requirement will already have been met. These joint consents are the only type of consent by which one covered entity can obtain the individual's permission for another covered entity to use or disclose protected health information to carry out treatment, payment, or health care operations.

Effect of Consent

These consents, as well as the authorizations described in § 164.508, should not be construed to waive, directly or indirectly, any privilege granted under federal, state, or local law or procedure. Consents obtained under this regulation are not appropriate for the disposition of more technical and legal proceedings and may not comport with procedures and standards of federal, state, or local judicial practice. For example, state courts and other decision-making bodies may choose to examine more closely the circumstances and propriety of such consent and may adopt more protective standards for application in their proceedings. In the judicial setting, as in the legislative and executive settings, states may provide for greater protection of privacy. Additionally, both the Congress and the Secretary have established a general approach to protecting from explicit preemption state laws that are more protective of privacy than the protections set forth in this regulation.

Section 164.508—Uses and Disclosures for Which an Authorization Is Required

Section 164.508(a)—Standard

We proposed to require covered entities to obtain the individual's authorization for all uses and disclosures of protected health information not otherwise permitted or required under the proposed rule. Uses and disclosures that would have been permitted without individual authorization included uses and disclosures for national priority purposes such as public health, law enforcement, and research (see proposed § 164.510) and uses and disclosures of protected health information, other than psychotherapy notes and research information unrelated to treatment, for purposes of treatment, payment, and health care operations (see proposed § 164.506). We also proposed to require covered entities to disclose protected health information to the individual for inspection and copying (see proposed § 164.514) and to the Secretary as required for enforcement of the rule (see proposed § 164.522). Individual authorization would not have been required for these uses and disclosures.

We proposed to require covered entities to obtain the individual's authorization for all other uses and disclosures of protected health information. Under proposed § 164.508(a), uses and disclosures that would have required individual authorization included, but were not limited to, the following:

- Use for marketing of health and non-health items and services by the covered entity;
- Disclosure by sale, rental, or barter;
- Use and disclosure to non-health related divisions of the covered entity, e.g., for use in marketing life or casualty insurance or banking services;
- Disclosure, prior to an individual's enrollment in a health plan, to the health plan or health care provider for making eligibility or enrollment determinations relating to the individual or for underwriting or risk rating determinations;
- Disclosure to an employer for use in employment determinations; and
- Use or disclosure for fundraising.

In the preamble to the proposed rule, we stated that covered entities would be bound by the terms of authorizations. Uses or disclosures by the covered entity for purposes inconsistent with the statements made in the authorization would have constituted a violation of the rule.

In the final rule, under § 164.508(a), as in the proposed rule, covered entities must have authorization from individuals before using or disclosing protected health information for any purpose not otherwise permitted or required by this rule. Specifically, except for psychotherapy notes (see below), covered entities are not required to obtain the individual's authorization to use or disclose protected health information to carry out treatment, payment, and health care operations. (Covered entities may, however, be required to obtain the individual's consent for these uses and disclosures. See the preamble regarding § 164.506 for a discussion of ''consent'' versus ''authorization''.) We also do not require covered entities to obtain the individual's authorization for uses and disclosures of protected health information permitted under §§ 164.510 or 164.512, for disclosures to the individual, or for required disclosures to the Secretary under subpart C of part 160 of this subchapter for enforcement of this rule.

In the final rule, we clarify that covered entities are bound by the

statements provided on the authorization; use or disclosure by the covered entity for purposes inconsistent with the statements made in the authorization constitutes a violation of this rule.

Unlike the proposed rule, we do not include in the regulation examples of the types of uses and disclosures that require individual authorization. We eliminated two examples from the proposed list due to potential confusion as to our intent: disclosure by sale, rental, or barter and use and disclosure to non-health related divisions of the covered entity. We recognize that covered entities sometimes make these types of uses and disclosures for purposes that are permitted under the rule without authorization. For example, a covered health care provider may sell its accounts receivable to a collection agency for payment purposes and a health plan may disclose protected health information to its life insurance component for payment purposes. We do not intend to require authorization for uses and disclosures made by sale, rental, or barter or for disclosures made to non-health related divisions of the covered entity, if those uses or disclosures could otherwise be made without authorization under this rule. As with any other use or disclosure, however, uses and disclosures of protected health information for these purposes do require authorization if they are not otherwise permitted under the rule.

We also eliminated the remaining proposed examples from the final rule due to concern that these examples might be misinterpreted as an exhaustive list of all of the uses and disclosures that require individual authorization. We discuss the examples here, however, to clarify the interaction of the authorization requirements and the provisions of the rule that permit uses and disclosures without authorization and/or with consent. Uses and disclosures for which covered entities must have the individual's authorization include, but are not limited to, the following activities.

Marketing

As in the proposed rule, covered entities must obtain the individual's authorization before using or disclosing protected health information for marketing purposes. In the final rule, we add a new definition of marketing (see § 164.501). For more detail on what activities constitute marketing, see § 164.501, definition of ''marketing,'' and § 164.514(e).

Pre-Enrollment Underwriting

As in the proposed rule, covered entities must obtain the individual's authorization to use or disclose protected health information for the purpose of making eligibility or enrollment determinations relating to an individual or for underwriting or risk rating determinations, prior to the individual's enrollment in a health plan (that is, for purposes of pre-enrollment underwriting). For example, if an individual applies for new coverage with a health plan in the non-group market and the health plan wants to review protected health information from the individual's covered health care providers before extending an offer of coverage, the individual first must authorize the covered providers to share the information with the health plan. If the individual applies for renewal of existing coverage, however, the health plan would not need to obtain an authorization to review its existing claims records about that individual, because this activity would come within the definition of health care operations and be permissible. We also note that under § 164.504(f), a group health plan and a health insurance issuer that provides benefits with respect to a group health plan are permitted in certain circumstances to disclose summary health information to the plan sponsor for the purpose of obtaining premium bids. Because these disclosures fall within the definition of health care operations, they do not require authorization.

Employment Determinations

As in the proposed rule, covered entities must obtain the individual's authorization to use or disclose protected health information for employment determinations. For example, a covered health care provider must obtain the individual's authorization to disclose the results of a pre-employment physical to the individual's employer. The final rule provides that a covered entity may condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party on the provision of authorization for the disclosure of the information to the third party.

Fundraising

Under the proposed regulation, we would have required authorization before a covered entity could have used or disclosed protected health information for fundraising. In the final rule, we narrow the circumstances under which covered entities must obtain the individual's authorization to use or disclose protected health information for fundraising purposes. As provided in § 164.514(f) and described in detail in the corresponding preamble, authorization is not required when a covered entity uses or discloses demographic information and information about the dates of health care provided to an individual for the purpose of raising funds for its own benefit, nor when it discloses such information to an institutionally related foundation to raise funds for the covered entity.

Any use or disclosure for fundraising purposes that does not meet the requirements of § 164.514(f) and does not fall within the definition of health care operations (see § 164.501), requires authorization. Specifically, covered entities must obtain the individual's authorization to use or disclose protected health information to raise funds for any entity other than the covered entity. For example, a covered entity must have the individual's authorization to use protected health information about the individual to solicit funds for a non-profit organization that engages in research, education, and awareness efforts about a particular disease.

Psychotherapy Notes

In the NPRM, we proposed different rules with respect to psychotherapy notes than we proposed with respect to all other protected health information. The proposed rule would have required covered entities to obtain an authorization for any use or disclosure of psychotherapy notes to carry out treatment, payment, or health care operations, unless the use was by the person who created the psychotherapy notes. With respect to all other protected health information, we proposed to prohibit covered entities from requiring authorization for uses and disclosures for these purposes.

We significantly revise our approach to psychotherapy notes in the final rule. With a few exceptions, covered entities must obtain the individual's authorization to use or disclose psychotherapy notes to carry out treatment, payment, or health care operations. A covered entity must obtain the individual's consent, but not an authorization, for the person who created the psychotherapy notes to use the notes to carry out treatment and for the covered entity to use or disclose psychotherapy notes for conducting training programs in which students, trainees, or practitioners in mental health learn under supervision to

practice or improve their skills in group, joint, family, or individual counseling. A covered entity may also use psychotherapy notes to defend a legal action or other proceeding brought by the individual pursuant to a consent, without a specific authorization. We note that, while this provision allows disclosure of these records to the covered entity's attorney to defend against the action or proceeding, disclosure to others in the course of a judicial or administrative proceeding is governed by § 164.512(e). This special provision is necessary because disclosure of protected health information for purposes of legal representatives may be made under the general consent as part of ''health care operations.'' Because we require an authorization for disclosure of psychotherapy notes for ''health care operations,'' an exception is needed to allow covered entities to use protected health information about an individual to defend themselves against an action threatened or brought by that individual without asking that individual for authorization to do so. Otherwise, a consent under § 164.506 is not sufficient for the use or disclosure of psychotherapy notes to carry out treatment, payment, or health care operations. Authorization is required. We anticipate these authorizations will rarely be necessary, since psychotherapy notes do not include information that covered entities typically need for treatment, payment, or other types of health care operations.

In the NPRM, we proposed to permit covered entities to use and disclose psychotherapy notes for all other purposes permitted or required under the rule without authorization. In the final rule, we specify a more limited set of uses and disclosures of psychotherapy notes that covered entities are permitted to make without authorization. An authorization is not required for use or disclosure of psychotherapy notes when required for enforcement purposes, in accordance with subpart C of part 160 of this subchapter; when mandated by law, in accordance with § 164.512(a); when needed for oversight of the health care provider who created the psychotherapy notes, in accordance with § 164.512(d); when needed by a coroner or medical examiner, in accordance with § 164.512(g)(1); or when needed to avert a serious and imminent threat to health or safety, in accordance with § 164.512(j)(1)(i). We also provide transition provisions in § 164.532 regarding the effect of express legal permission obtained from an individual prior to the compliance date of this rule.

Section 164.508(b)—Implementation Specifications for Authorizations

Valid and Defective Authorizations

We proposed to require a minimum set of elements for authorizations requested by the individual and an additional set of elements for authorizations requested by a covered entity. We would have permitted covered entities to use and disclose protected health information pursuant to authorizations containing the applicable required elements. We would have prohibited covered entities from acting on an authorization if the submitted document had any of the following defects:

- The expiration date had passed;
- The form had not been filled out completely;
- The covered entity knew the authorization had been revoked;
- The completed form lacked a required element; or
- The covered entity knew the information on the form was false.

In § 164.508(b)(1) of the final rule, we specify that an authorization containing the applicable required elements (as described below) is a valid authorization. We clarify that a valid authorization may contain additional, non-required elements, provided that these elements are not inconsistent with the required elements. Covered entities are not required to use or disclose protected health information pursuant to a valid authorization. Our intent is to clarify that a covered entity that uses or discloses protected health information pursuant to an authorization meeting the applicable requirements will be in compliance with this rule.

We retain the provision prohibiting covered entities from acting on an authorization if the submitted document had any of the listed defects, with a few changes. First, in § 164.508(c)(1)(iv) we specify that an authorization may expire upon a certain event or on a specific date. For example, a valid authorization may state that it expires upon acceptance or rejection of an application for insurance or upon the termination of employment (for example, in an authorization for disclosure of protected health information for fitness-for-duty purposes) or similar event. The expiration event must, however, be related to the individual or the purpose of the use or disclosure. An authorization that purported to expire on the date when the stock market reached a specified level would not be valid. Under § 164.508(b)(2)(i), if the expiration event is known by the covered entity to have occurred, the authorization is defective. Second, we clarify that certain compound authorizations, as described below, are defective. We also clarify that authorizations that are not completely filled out with respect to the required elements are defective. Finally, we clarify that an authorization with information that the covered entity knows to be false is defective only if the information is material.

As under the proposed regulation, an authorization that the covered entity knows has been revoked is not a valid authorization. We note that, although an authorization must be revoked in writing, the covered entity may not always ''know'' that an authorization has been revoked. The writing required for an individual to revoke an authorization may not always trigger the ''knowledge'' required for a covered entity to consider an authorization defective. Conversely, a copy of the written revocation is not required before a provider ''knows'' that an authorization has been revoked.

Many authorizations will be obtained by persons other than the covered entity. If the individual revokes an authorization by writing to that other person, and neither the individual nor the other person informs the covered entity of the revocation, the covered entity will not ''know'' that the authorization has been revoked. For example, a government agency may obtain an individual's authorization for ''all providers who have seen the individual in the past year'' to disclose protected health information to the agency for purposes of determining eligibility for benefits. The individual may revoke the authorization by writing to the government agency requesting such revocation. We cannot require the agency to inform all covered entities to whom it has presented the authorization that the authorization has been revoked. If a covered entity does not know of the revocation, the covered entity will not violate this rule by acting pursuant to the authorization. At the same time, if the individual does inform the covered entity of the revocation, even orally, the covered entity ''knows'' that the authorization has been revoked and can no longer treat the authorization as valid under this rule. Thus, in this example, if the individual tells a covered entity that the individual has revoked the authorization, the covered entity ''knows'' of the revocation and must consider the authorization defective under § 164.508(b)(2).

Compound Authorizations

Except for authorizations requested in connection with a clinical trial, we proposed to prohibit covered entities from combining an authorization for use or disclosure of protected health information for purposes other than treatment, payment, or health care operations with an authorization or consent for treatment (*e.g.,* an informed consent to receive care) or payment (*e.g.,* an assignment of benefits).

We clarify the prohibition on compound authorizations in the final rule. Other than as described below, § 164.508(b)(3) prohibits a covered entity from acting on an authorization required under this rule that is combined with any other document, including any other written legal permission from the individual. For example, an authorization under this rule may not be combined with a consent for use or disclosure of protected health information under § 164.506, with the notice of privacy practices under § 164.520, with any other form of written legal permission for the use or disclosure of protected health information, with an informed consent to participate in research, or with any other form of consent or authorization for treatment or payment.

There are three exceptions to this prohibition. First, under § 164.508(f) (described in more detail, below), an authorization for the use or disclosure of protected health information created for research that includes treatment of the individual may be combined with a consent for the use or disclosure of that protected health information to carry out treatment, payment, or health care operations under § 164.506 and with other documents as provided in § 164.508(f). Second, authorizations for the use or disclosure of psychotherapy notes for multiple purposes may be combined in a single document, but may not be combined with authorizations for the use or disclosure of other protected health information. Third, authorizations for the use or disclosure of protected health information other than psychotherapy notes may be combined, provided that the covered entity has not conditioned the provision of treatment, payment, enrollment, or eligibility on obtaining the authorization. If a covered entity conditions any of these services on obtaining an authorization from the individual, as permitted in § 164.508(b)(4) and described below, the covered entity must not combine the authorization with any other document.

The following are examples of valid compound authorizations: an authorization for the disclosure of information created for clinical research combined with a consent for the use or disclosure of other protected health information to carry out treatment, payment, and health care operations, and the informed consent to participate in the clinical research; an authorization for disclosure of psychotherapy notes for both treatment and research purposes; and an authorization for the disclosure of the individual's demographic information for both marketing and fundraising purposes. Examples of invalid compound authorizations include: an authorization for the disclosure of protected health information for treatment, for research, and for determining payment of a claim for benefits, when the covered entity will refuse to pay the claim if the individual does not sign the authorization; or an authorization for the disclosure of psychotherapy notes combined with an authorization to disclose any other protected health information.

Prohibition on Conditioning Treatment, Payment, Eligibility, or Enrollment

We proposed to prohibit covered entities from conditioning treatment or payment on the provision by the individual of an authorization, except when the authorization was requested in connection with a clinical trial. In the case of authorization for use or disclosure of psychotherapy notes or research information unrelated to treatment, we proposed to prohibit covered entities from conditioning treatment, payment, or enrollment in a health plan on obtaining such an authorization.

We retain this basic approach but refine its application in the final rule. In addition to the general prohibition on conditioning treatment and payment, covered entities are also prohibited (with certain exceptions described below) from conditioning eligibility for benefits or enrollment in a health plan on obtaining an authorization. This prohibition extends to all authorizations, not just authorizations for use or disclosure of psychotherapy notes. This prohibition is intended to prevent covered entities from coercing individuals into signing an authorization for a use or disclosure that is not necessary to carry out the primary services that the covered entity provides to the individual. For example, a health care provider could not refuse to treat an individual because the individual refused to authorize a disclosure to a pharmaceutical manufacturer for the purpose of marketing a new product.

We clarify the proposed research exception to this prohibition. Covered entities seeking authorization in accordance with § 164.508(f) to use or disclose protected health information created for the purpose of research that includes treatment of the individual, including clinical trials, may condition the research-related treatment on the individual's authorization. Permitting use of protected health information is part of the decision to receive care through a clinical trial, and health care providers conducting such trials should be able to condition research-related treatment on the individual's willingness to authorize the use or disclosure of his or her protected health information for research associated with the trial.

In addition, we permit health plans to condition eligibility for benefits and enrollment in the health plan on the individual's authorization for the use or disclosure of protected health information for purposes of eligibility or enrollment determinations relating to the individual or for its underwriting or risk-rating determinations. We also permit health plans to condition payment of a claim for specified benefits on the individual's authorization for the disclosure of information maintained by another covered entity to the health plan, if the disclosure is necessary to determine payment of the claim. These exceptions do not apply, however, to authorization for the use or disclosure of psychotherapy notes. Health plans may not condition payment, eligibility, or enrollment on the receipt of an authorization for the use or disclosure of psychotherapy notes, even if the health plan intends to use the information for underwriting or payment purposes.

Finally, when a covered entity provides treatment for the sole purpose of providing information to a third party, the covered entity may condition the treatment on the receipt of an authorization to use or disclose protected health information related to that treatment. For example, a covered health care provider may have a contract with an employer to provide fitness-for-duty exams to the employer's employees. The provider may refuse to conduct the exam if an individual refuses to authorize the provider to disclose the results of the exam to the employer. Similarly, a covered health care provider may have a contract with a life insurer to provide pre-enrollment physicals to applicants for life insurance coverage. The provider may refuse to conduct the physical if an individual refuses to authorize the provider to disclose the results of the physical to the life insurer.

Revocation of Authorizations

We proposed to allow individuals to revoke an authorization at any time, except to the extent that the covered entity had taken action in reliance on the authorization.

We retain this provision, but specify that the individual must revoke the authorization in writing. When an individual revokes an authorization, a covered entity that knows of such revocation must stop making uses and disclosures pursuant to the authorization to the greatest extent practical. A covered entity may continue to use and disclose protected health information in accordance with the authorization only to the extent the covered entity has taken action in reliance on the authorization. For example, a covered entity is not required to retrieve information that it has already disclosed in accordance with the authorization. (See above for discussion of how written revocation of an authorization and knowledge of that revocation may differ.)

We also include an additional exception. Under § 164.508(b)(5), individuals do not have the right to revoke an authorization if the authorization was obtained as a condition of obtaining insurance coverage and other applicable law provides the insurer that obtained the authorization with the right to contest a claim under the policy. We intend this exception to permit insurers to obtain necessary protected health information during contestability periods under state law. For example, an individual may not revoke an authorization for the disclosure of protected health information to a life insurer for the purpose of investigating material misrepresentation if the individual's policy is still subject to the contestability period.

Documentation

In the final rule, we clarify that a covered entity must document and retain any signed authorization as required by § 164.530(j) (see below).

Section 164.508(c)—Core Elements and Requirements

We proposed to require authorizations requested by individuals to contain a minimum set of elements: a description of the information to be used or disclosed; the name of the covered entity, or class of entities or persons, authorized to make the use or disclosure; the name or types of recipient(s) of the information; an expiration date; the individual's signature and date of signature; if signed by a representative, a description of the representative's authority or relationship to the individual; a statement regarding the individual's right to revoke the authorization; and a statement that the information may no longer be protected by the federal privacy law. We proposed a model authorization form that entities could have used to satisfy the authorization requirements. If the model form was not used, we proposed to require covered entities to use authorization forms written in plain language.

We modify the proposed approach, by eliminating the distinction between authorizations requested by the individuals and authorizations requested by others. Instead, we prescribe a minimum set of elements for authorizations and certain additional elements when the authorization is requested by a covered entity for its own use or disclosure of protected health information it maintains or for receipt of protected health information from another covered entity to carry out treatment, payment, or health care operations.

The core elements are required for all authorizations, not just authorizations requested by individuals. Individuals seek disclosure of protected health information about them to others in many circumstances, such as when applying for life or disability insurance, when government agencies conduct suitability investigations, and in seeking certain job assignments when health status is relevant. Another common instance is tort litigation, when an individual's attorney needs individually identifiable health information to evaluate an injury claim and asks the individual to authorize disclosure of records relating to the injury to the attorney. In each of these situations, the individual may go directly to the covered entity and ask it to send the relevant information to the intended recipient. Alternatively, the intended recipient may ask the individual to complete a form, which the recipient will submit to the covered entity on the individual's behalf, that authorizes the covered entity to disclose the information. Whether the authorization is submitted to the covered entity by the individual or by another person on the individual's behalf, the covered entity maintaining protected health information may not use or disclose it pursuant to an authorization unless the authorization meets the following requirements.

First, the authorization must include a description of the information to be used or disclosed, with sufficient specificity to allow the covered entity to know which information the authorization references. For example, the authorization may include a description of ''laboratory results from July 1998'' or ''all laboratory results'' or ''results of MRI performed in July 1998.'' The covered entity can then use or disclose that information and only that information. If the covered entity does not understand what information is covered by the authorization, the use or disclosure is not permitted unless the covered entity clarifies the request.

There are no limitations on the information that can be authorized for disclosure. If an individual wishes to authorize a covered entity to disclose his or her entire medical record, the authorization can so specify. In order for the covered entity to disclose the entire medical record, the authorization must be specific enough to ensure that the individual has a clear understanding that the entire record will be disclosed. For example, if the Social Security Administration seeks authorization for release of all health information to facilitate the processing of benefit applications, then the description on the authorization form must specify ''all health information'' or the equivalent.

In some instances, a covered entity may be reluctant to undertake the effort to review the record and select portions relevant to the request (or redact portions not relevant). In such circumstances, covered entities may provide the entire record to the individual, who may then redact and release the more limited information to the requestor. This rule does not require a covered entity to disclose information pursuant to an individual's authorization.

Second, the authorization must include the name or other specific identification of the person(s) or class of persons that are authorized to use or disclose the protected health information. If an authorization permits a class of covered entities to disclose information to an authorized person, the class must be stated with sufficient specificity so that a covered entity presented with the authorization will know with reasonable certainty that the individual intended the covered entity to release protected health information. For example, a covered licensed nurse practitioner presented with an authorization for ''all physicians'' to disclose protected health information could not know with reasonable certainty that the individual intended for the practitioner to be included in the authorization.

Third, the authorization must include the name or other specific identification of the person(s) or class of persons to

whom the covered entity is authorized to make the use or disclosure. The authorization must identify these persons with sufficient specificity to reasonably permit a covered entity responding to the authorization to identify the authorized user or recipient of the protected health information. Often, individuals provide authorizations to third parties, who present them to one or more covered entities. For example, an authorization could be completed by an individual and given to a government agency, authorizing the agency to receive medical information from any health care provider that has treated the individual within a defined period of time. Such an authorization is permissible (subject to the other requirements of this part) if it sufficiently identifies the government entity that is authorized to receive the disclosed protected health information.

Fourth, the authorization must state an expiration date or event. This expiration date or event must either be a specific date (*e.g.,* January 1, 2001), a specific time period (*e.g.,* one year from the date of signature), or an event directly relevant to the individual or the purpose of the use or disclosure (*e.g.,* for the duration of the individual's enrollment with the health plan that is authorized to make the use or disclosure). We note that the expiration date or event is subject to otherwise applicable and more stringent law. For example, the National Association of Insurance Commissioners' Insurance Information and Privacy Protection Model Act, adopted in at least fifteen states, specifies that authorizations signed for the purpose of collecting information in connection with an application for a life, health, or disability insurance policy are permitted to remain valid for no longer than thirty months. In those states, the longest such an authorization may remain in effect is therefore thirty months, regardless of the expiration date or event indicated on the form.

Fifth, the authorization must state that the individual has the right to revoke an authorization in writing, except to the extent that action has been taken in reliance on the authorization or, if applicable, during a contestability period. The authorization must include instructions on how the individual may revoke the authorization. For example, the person obtaining the authorization from the individual can include an address where the individual can send a written request for revocation.

Sixth, the authorization must inform the individual that, when the information is used or disclosed pursuant to the authorization, it may be subject to re-disclosure by the recipient and may no longer be protected by this rule.

Seventh, the authorization must include the individual's signature and the date of the signature. Once we adopt the standards for electronic signature, another of the required administrative simplification standards we are required to adopt under HIPAA, an electronic signature that meets those standards will be sufficient under this rule. We do not require verification of the individual's identity or authentication of the individual's signature.

Finally, if the authorization is signed by a personal representative of the individual, the representative must indicate his or her authority to act for the individual.

As in the proposed rule, the authorization must be written in plain language. See the preamble discussion regarding notice of privacy practices (§ 164.520) for a discussion of the plain language requirement. We do not provide a model authorization in this rule. We will provide further guidance on this issue prior to the compliance date.

Section 164.508(d)—Authorizations Requested by a Covered Entity for Its Own Uses and Disclosures

We proposed to require covered entities to include additional elements in authorizations initiated by the covered entity. Before a covered entity could use or disclose protected health information of an individual pursuant to a request the covered entity made, we proposed to require the entity to obtain an authorization containing the minimum elements described above and the following additional elements: except for authorizations requested for clinical trials, a statement that the entity will not condition treatment or payment on the individual's authorization; a description of the purpose of the requested use or disclosure; a statement that the individual may inspect or copy the information to be used or disclosed and may refuse to sign the authorization; and, if the use or disclosure of the requested information will result in financial gain to the entity, a statement that such gain will result.

We additionally proposed to require covered entities, when requesting an individual's authorization, to request only the minimum amount of information necessary to accomplish the purpose for which the request was made. We also proposed to require covered entities to provide the individual with a copy of the executed authorization.

We retain the proposed approach, but apply these additional requirements when the covered entity requests the individual's authorization for the entity's own use or disclosure of protected health information maintained by the covered entity itself. For example, a health plan may ask individuals to authorize the plan to disclose protected health information to a subsidiary to market life insurance to the individual. A pharmaceutical company may also ask a covered provider to recruit patients for drug research; if the covered provider asks patients to sign an authorization for the provider to disclose protected health information to the pharmaceutical company for this research, this is also an authorization requested by a covered entity for disclosure of protected health information maintained by the covered entity. When covered entities initiate the authorization by asking individuals to authorize the entity to use or disclose protected health information that the entity maintains, the authorization must include all of the elements required above as well as several additional elements.

Authorizations requested by covered entities for the covered entity's own use or disclosure of protected health information must state, as applicable under § 164.508(b)(4), that the covered entity will not condition treatment, payment, enrollment, or eligibility on the individual's authorization for the use or disclosure. For example, if a health plan asks an individual to sign an authorization for the health plan to disclose protected health information to a non-profit advocacy group for the advocacy group's fundraising purposes, the authorization must contain a statement that the health plan will not condition treatment, payment, enrollment in the health plan, or eligibility for benefits on the individual providing the authorization.

Authorizations requested by covered entities for their own uses and disclosures of protected health information must also identify each purpose for which the information is to be used or disclosed. The required statement of purpose(s) must provide individuals with the facts they need to make an informed decision whether to allow release of the information. We prohibit the use of broad or blanket authorizations requesting the use or disclosure of protected health information for a wide range of unspecified purposes. Both the information that is to be used or disclosed and the specific purpose(s) for such uses or disclosures must be stated in the authorization.

Authorizations requested by covered entities for their own uses and disclosures must also advise individuals of certain rights available to them under this rule. The authorization must state that the individual may inspect or copy the information to be used or disclosed as provided in § 164.524 regarding access for inspection and copying and that the individual may refuse to sign the authorization.

We alter the proposed requirements with respect to authorizations for which the covered entity will receive financial gain. When the covered entity initiates the authorization and the covered entity will receive direct or indirect remuneration from a third party (rather than financial gain, as proposed) in exchange for using or disclosing the protected health information, the authorization must include a statement that such remuneration will result. For example, a health plan may wish to sell or rent its enrollee mailing list or a pharmaceutical company may offer a covered provider a discount on its products if the provider obtains authorization to disclose the demographic information of patients with certain diagnoses so that the company can market new drugs to them directly. In each case, the covered entity must obtain the individual's authorization, and the authorization must include a statement that the covered entity will receive remuneration.

In § 164.508(d)(2), we continue to require a covered entity that requests an authorization for its own use or disclosure of protected health information to provide the individual with a copy of the signed authorization. While we eliminate from this section the provision requiring covered entities to obtain authorization for use or disclosure of the minimum necessary protected health information, § 164.514(d)(4) requires covered entities to request only the minimum necessary protected health information to accomplish the purpose for which the request is made. This requirement applies to these authorizations, as well as other requests.

Section 164.508(e)—Authorizations Requested by a Covered Entity for Disclosures by Others

In the proposed rule, we would have prohibited all covered entities from requiring the individual's written legal permission (as proposed, an ''authorization'') for the use or disclosure of protected health information to carry out treatment, payment, or health care operations. We generally eliminate this prohibition in the final rule, except to specify that a consent obtained by one covered entity is not effective to permit another covered entity to use or disclose protected health information. See § 164.506(a)(5) and the corresponding preamble discussion.

In the final rule, if a covered entity seeks the individual's written legal permission to obtain protected health information about the individual from another covered entity for any purpose, it must obtain the individual's authorization for the covered entity that maintains the protected health information to make the disclosure. If the authorization is for the purpose of obtaining protected health information for purposes other than treatment, payment, or health care operations, the authorization need only contain the core elements required by § 164.508(c) and described above.

If the authorization, however, is for the purpose of obtaining protected health information to carry out treatment, payment, or health care operations, the authorization must meet the requirements of § 164.508(e). We expect such authorizations will rarely be necessary, because we expect covered entities that maintain protected health information to obtain consents that permit them to make anticipated uses and disclosures for these purposes. An authorization obtained by another covered entity that authorizes the covered entity maintaining the protected health information to make a disclosure for the same purpose, therefore, would be unnecessary.

We recognize, however, that these authorizations may be useful to demonstrate an individual's intent and relationship to the intended recipient of the information when the intent or relationship is not already clear. For example, a long term care insurer may need information from an individual's health care providers about the individual's ability to perform activities of daily living in order to determine payment of a long term care claim. The providers that hold the information may not be providing the long term care and may not, therefore, be aware of the individual's coverage under the policy or that the individual is receiving long term care services. An authorization obtained by the long term care insurer will help to demonstrate these facts to the providers holding the information, which will make them more confident that the individual intends for the information to be shared. Similarly, an insurer with subrogation obligations may need health information from the enrollee's providers to assess or prosecute the claim. A patient's new physician may also need medical records from the patient's prior providers in order to treat the patient. Without an authorization that demonstrates the patient's intent for the information to be shared, the covered entity that maintains the protected health information may be reluctant to provide the information, even if that covered entity's consent permits such disclosure to occur.

These authorizations may also be useful to accomplish clinical coordination and integration among covered entities that do not meet the definitions of affiliated covered entities or organized health care arrangements. For example, safety-net providers that participate in the Community Access Program (CAP) may not qualify as organized health care arrangements but may want to share protected health information with each other in order to develop and expand integrated systems of care for uninsured people. An authorization under this section would permit such providers to receive protected health information from other CAP participants to engage in such activities.

Because of such concerns, we permit a covered entity to request the individual's authorization to obtain protected health information from another covered entity to carry out treatment, payment, and health care operations. In these situations, the authorization must contain the core elements described above and must also describe each purpose of the requested disclosure.

With one exception, the authorization must also indicate that the authorization is voluntary. It must state that the individual may refuse to sign the authorization and that the covered entity requesting the authorization will not condition the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits on obtaining the individual's authorization. If the authorization is for a disclosure of information that is necessary to determine payment of a claim for specified benefits, however, the health plan requesting the authorization may condition the payment of the claim on obtaining the authorization from the individual. See § 164.508(b)(4)(iii). In this case, the authorization does not have to state that the health plan will not condition payment on obtaining the authorization.

The covered entity requesting the authorization must provide the individual with a copy of the signed authorization. We note that the covered entity requesting the authorization is also subject to the requirements in

§ 164.514 to request only the minimum necessary information needed for the purpose of the authorization.

We additionally note that, when the covered entity that maintains the protected health information has already obtained a consent for disclosure of protected health information to carry out treatment, payment, and/or health care operations under § 164.506, and that consent conflicts with an authorization obtained by another covered entity under § 164.508(e), the covered entity maintaining the protected health information is bound by the more restrictive document. See § 164.506(e) and the corresponding preamble discussion for further explanation.

Section 164.508(f)—Authorizations for Uses and Disclosures of Protected Health Information Created for Research that Includes Treatment of Individuals

In the proposed rule, we would have required individual authorization for any use or disclosure of research information unrelated to treatment. In the final rule, we eliminate the special rules for this category of information and, instead, require covered entities to obtain an authorization for the use or disclosure of protected health information the covered entity creates for the purpose of research that includes treatment of individuals, except as otherwise permitted by § 164.512(i).

The intent of this provision is to permit covered entities that conduct research involving treatment to bind themselves to a more limited scope of uses and disclosures of research information than they would otherwise be permitted to make with non-research information. Rather than creating a single definition of ''research information,'' we allow covered entities the flexibility to define that subset of protected health information they create during clinical research that is not necessary for treatment, payment, or health care operations and that the covered entity will use or disclose under more limited circumstances than it uses or discloses other protected health information. In designing their authorizations, we expect covered entities to be mindful of the often highly sensitive nature of research information and the impact of individuals' privacy concerns on their willingness to participate in research.

Covered entities seeking authorization to use or disclose protected health information they create for the purpose of research that includes treatment of individuals, including clinical trials, must include in the authorization (in addition to the applicable elements required above) a description of the extent to which some or all of the protected health information created for the research will also be used or disclosed for purposes of treatment, payment, and health care operations. For example, if the covered entity intends to seek reimbursement from the individual's health plan for the routine costs of care associated with the research protocol, it must explain in the authorization the types of information that it will provide to the health plan for this purpose. This information, and the circumstances under which disclosures will be made for treatment, payment, and health care operations, may be more limited than the information and circumstances described in the covered entity's general consent and notice of privacy practices. To the extent the covered entity limits itself to a subset of uses or disclosures that are otherwise permissible under the rule and the covered entity's consent and notice, the covered entity is bound by the statements made in the research-related authorization. In these circumstances, the authorization must indicate that the authorization, not the general consent and notice, controls.

If the covered entity's primary interaction with the individual is through the research, the covered entity may combine the general consent for treatment, payment, and health care operations required under § 164.506 with this research authorization and need not obtain an additional consent under § 164.506. If the entity has already obtained, or intends to obtain, a separate consent as required under § 164.506, the research authorization must refer to that consent and state that the practices described in the research-related authorization are binding on the covered entity as to the information covered by the research-related authorization. The research-related authorization may also be combined in the same document as the informed consent for participation in the research. This is an exception to the general rule in § 164.508(b)(3) that an authorization under this section may not be combined with any other document (see above).

The covered entity must also include in the authorization a description of the extent to which it will not use or disclose the protected health information it obtains in connection with the research protocol for purposes that are permitted without individual authorization under this rule (under §§ 164.510 and 164.512). To the extent that the entity limits itself to a subset of uses or disclosures that are otherwise permissible under the rule and the entity's notice, the entity is bound by the statements made in the research authorization. In these circumstances, the authorization must indicate that the authorization, not the notice, controls. The covered entity may not, however, purport to preclude itself from making uses or disclosures that are required by law or that are necessary to avert a serious and imminent threat to health or safety.

In some instances, the covered entity may wish to make a use or disclosure of the research information that it did not include in its general consent or notice or for which authorization is required under this rule. To the extent the entity includes uses or disclosures in the research authorization that are otherwise not permissible under the rule and the entity's consent and notice of information practices, the entity must include all of the elements required by §§ 164.508(c) and (d) in the research-related authorization. The covered entity is bound by these statements.

Research that involves the delivery of treatment to participants sometimes relies on existing health information, such as to determine eligibility for the trial. We note that under § 164.508(b)(3)(iii), the covered entity may combine the research-related authorization required under § 164.508(f) with any other authorization for the use or disclosure of protected health information (other than psychotherapy notes), provided that the covered entity does not condition the provision of treatment on the individual signing the authorization. For example, a covered health care provider that had a treatment relationship with an individual prior to the individual's enrollment in a clinical trial, but that is now providing research-related treatment to the individual, may elect to request a compound authorization from the individual: an authorization under § 164.508(d) for the provider to use the protected health information it created prior to the initiation of the research that involves treatment, combined with an authorization under § 164.508(f) regarding use and disclosure of protected health information the covered provider will create for the purpose of the clinical trial. This compound authorization would be valid, provided the covered provider did not condition the research-related treatment on obtaining the authorization required under § 164.508(f), as permitted in § 164.508(b)(4)(i).

However, we anticipate that covered entities will almost always, if not always, condition the provision of research-related treatment on the individual signing the authorization under § 164.508(f) for the covered

entity's use or disclosure of protected health information created for the research. Therefore, we expect that the vast majority of covered providers who wish to use or disclose protected health information about an individual that will be created for research that includes treatment and wish to use existing protected health information about that individual for the research that includes treatment, will be required to obtain two authorizations from the individual: (1) an authorization for the use and disclosure of protected health information to be created for the research that involves treatment of the individual (as required under § 164.508(f)), and (2) an authorization for the use of existing protected health information for the research that includes treatment of the individual (as required under § 164.508(d)).

Effect of Authorization

As noted in the discussion about consents in the preamble to § 164.506, authorizations under this rule should not be construed to waive, directly or indirectly, any privilege granted under federal, state, or local laws or procedures.

Section 164.510—Uses and Disclosures Requiring an Opportunity for the Individual To Agree or To Object

Introduction

Section 164.510 of the NPRM proposed the uses and disclosures of protected health information that covered entities could make for purposes other than treatment, payment, or health care operations and for which an individual authorization would not have been required. These allowable uses and disclosures were designed to permit and promote key national health care priorities, and to promote the smooth operation of the health care system. In each of these areas, the proposal permitted, but would not have required, covered entities to use or disclose protected health information.

We proposed to require covered entities to obtain the individual's oral agreement before making a disclosure to a health care facility's directory or to the individual's next-of-kin or to another person involved in the individual's health care. Because there is an expectation in these two areas that individuals will have some input into a covered entity's decision to use or disclose protected health information, we decided to place disclosures to health facility directories and to persons involved in an individual's care in a separate section. In the final rule, requirements regarding disclosure of protected health information for facility directories and to others involved in an individual's care are included in § 164.510(a) and § 164.510(b), respectively. In the final rule, we include in § 164.510(b) provisions to address a type of disclosure not addressed in the NPRM: disclosures to entities providing relief and assistance in disasters such as floods, fires, and terrorist attacks. Requirements for most of the remaining categories of disclosures addressed in proposed § 164.510 of the NPRM are included in a new § 164.512 of the final rule, as discussed below.

Section 164.510 of the final rule addresses situations in which the interaction between the covered entity and the individual is relatively informal and agreements are made orally, without written authorizations for use or disclosure. In general, under the final rule, to disclose or use protected health information for these purposes, covered entities must inform individuals in advance and must provide a meaningful opportunity for the individual to prevent or restrict the disclosure. In exceptional circumstances, where even this informal discussion cannot practicably take place, covered entities are permitted to make decisions regarding disclosure or use based on the exercise of professional judgment of what is in the individual's best interest.

Section 164.510(a)—Use and Disclosure for Facility Directories

The NPRM proposed to allow covered health care providers to disclose through an inpatient facility's directory a patient's name, location in the facility, and general health condition, provided that the individual had agreed to the disclosure. The NPRM would have allowed this agreement to be oral. Pursuant to the NPRM, when making decisions about incapacitated individuals, a covered health care provider could have disclosed such information at the entity's discretion and consistent with good medical practice and any prior expressions of patient preference of which the covered entity was aware.

The preamble to the NPRM listed several factors that we encouraged covered entities to take into account when making decisions about whether to include an incapacitated patient's information in the directory. These factors included: (1) Whether disclosing that an individual is in the facility could reasonably cause harm or danger to the individual (*e.g.,* if it appeared that an unconscious patient had been abused and disclosing the information could give the attacker sufficient information to seek out the person and repeat the abuse); (2) whether disclosing a patient's location within a facility implicitly would give information about the patient's condition (*e.g.,* whether a patient's room number revealed that he or she was in a psychiatric ward); (3) whether it was necessary or appropriate to give information about patient status to family or friends (*e.g.,* if giving information to a family member about an unconscious patient could help a physician administer appropriate medications); and (4) whether an individual had, prior to becoming incapacitated, expressed a preference not to be included in the directory. The preamble stated that if a covered entity learned of such a preference, it would be required to act in accordance with the preference.

The preamble to the NPRM said that when individuals entered a facility in an incapacitated state and subsequently gained the ability to make their own decisions, health facilities should ask them within a reasonable time period for permission to include their information in the facility's directory.

In the final rule, we change the NPRM's opt-in authorization requirement to an opt-out approach for inclusion of patient information in a health care facility's directory. The final rule allows covered health care providers—which in this case are health care facilities—to include patient information in their directory only if: (1) They inform incoming patients of their policies regarding the directory; (2) they give patients a meaningful opportunity to opt out of the directory listing or to restrict some or all of the uses and disclosures that can be included in the directory; and (3) the patient does not object to being included in the directory. A patient must be allowed, for example, to have his or her name and condition included in the directory while not having his or her religious affiliation included. The facility's notice and the individual's opt-out or restriction may be oral.

Under the final rule, subject to the individual's right to object, or known prior expressed preferences, a covered health care provider may disclose the following information to persons who inquire about the individual by name: (1) The individual's general condition in terms that do not communicate specific medical information about the individual (*e.g.,* fair, critical, stable, *etc.*); and (2) location in the facility. This approach represents a slight change to the NPRM, which did not require members of the general public to ask for a patient by name in order to obtain directory information and which,

in fact, would have allowed covered entities to disclose the individual's name as part of directory information.

Under the final rule, we also establish provisions for disclosure of directory information to clergy that are slightly different from those which apply for disclosure to the general public. Subject to the individual's right to object or restrict the disclosure, the final rule permits a covered entity to disclose to a member of the clergy: (1) The individual's name; (2) the individual's general condition in terms that do not communicate specific medical information about the individual; (3) the individual's location in the facility; and (4) the individual's religious affiliation. A disclosure of directory information may be made to members of the clergy even if they do not inquire about an individual by name. We note that the rule in no way requires a covered health care provider to inquire about the religious affiliation of an individual, nor must individuals supply that information to the facility. Individuals are free to determine whether they want their religious affiliation disclosed to clergy through facility directories.

We believe that allowing clergy to access patient information pursuant to this section does not violate the Establishment Clause of the First Amendment, which prohibits laws ''respecting an establishment of religion.'' Courts traditionally turn to the Lemon test when evaluating laws that might raise Establishment Clause concerns. A law does not violate the Clause if it has a secular purpose, is not primarily to advance religion, and does not cause excessive government entanglement with religion. The privacy regulation passes this test because its purpose is to protect the privacy of individuals—regardless of their religious affiliation—and it does not cause excessive government entanglement.

More specifically, although this section provides a special rule for members of the clergy, it does so as an accommodation to patients who seek to engage in religious conduct. For example, restricting the disclosure of an individual's religious affiliation, room number, and health status to a priest could cause significant delay that would inhibit the ability of a Catholic patient to obtain sacraments provided during the last rites. We believe this accommodation does not violate the Establishment Clause, because it avoids a government-imposed restriction on the disclosure of information that could disproportionately affect the practice of religion. In that way, it is no different from accommodations upheld by the U.S. Supreme Court, such as exceptions to laws banning the use of alcohol in religious ceremonies.

The final rule expands the circumstances under which health care facilities can disclose specified health information to the patient directory without the patient's agreement. Besides allowing such disclosures when patients are incapacitated, as the NPRM would have allowed, the final rule allows such disclosures in emergency treatment circumstances. For example, when a patient is conscious and capable of making a decision, but is so seriously injured that asking permission to include his or her information in the directory would delay treatment such that the patient's health would be jeopardized, health facilities can make decisions about including the patient's information in the directory according to the same rules that apply when the patient is incapacitated. The final rule modifies the NPRM requirements for cases in which an incapacitated patient is admitted to a health care facility. Whereas the NPRM would have allowed health care providers to disclose an incapacitated patient's information to the facility's directory ''at its discretion and consistent with good medical practice and any prior expressions of preference of which the covered entity [was] aware,'' the final rule states that in these situations (and in other emergency treatment circumstances), covered health care providers must make the decision on whether to include the patient's information in the facility's directory in accordance with professional judgment as to the patient's best interest. In addition, when making decisions involving incapacitated patients and patients in emergency situations, covered health care providers may decide to include some portions of the patient's information (such as name) but not other information (such as location in the facility) in order to protect patient interests.

As in the preamble to the NPRM, we encourage covered health care providers to take into account the four factors listed above when making decisions about whether to include patient information in a health care facility's directory when patients are incapacitated or are in an emergency treatment circumstance. In addition, we retain the requirement stated in the preamble of the NPRM that if a covered health care provider learns of an incapacitated patient's prior expression of preference not to be included in a facility's directory, the facility must not include the patient's information in the directory. For cases involving patients admitted to a health care facility in an incapacitated or emergency treatment circumstance who during the course of their stay become capable of decisionmaking, the final rule takes an approach similar to that described in the NPRM. The final rule states that when an individual who was incapacitated or in an emergency treatment circumstance upon admission to an inpatient facility and whose condition stabilizes such that he or she is capable of decisionmaking, a covered health care provider must, when it becomes practicable, inform the individual about its policies regarding the facility's directory and provide the opportunity to object to the use or disclosure of protected health information about themselves for the directory.

Section 164.510(b)—Uses and Disclosures for Involvement in the Individual's Care and Notification Purposes

In cases involving an individual with the capacity to make health care decisions, the NPRM would have allowed covered entities to disclose protected health information about the individual to a next-of-kin, to other family members, or to close personal friends of the individual if the individual had agreed orally to such disclosure. If such agreement could not practicably or reasonably be obtained (*e.g.,* when the individual was incapacitated), the NPRM would have allowed disclosure of protected health information that was directly relevant to the person's involvement in the individual's health care, consistent with good health professional practices and ethics. The NPRM defined next-of-kin as defined under state law.

Under the final rule, we specify that covered entities may disclose to a person involved in the current health care of the individual (such as a family member, other relative, close personal friend, or any other person identified by the individual) protected health information directly related to the person's involvement in the current health care of an individual or payment related to the individual's health care. Such persons involved in care and other contact persons might include, for example: blood relatives; spouses; roommates; boyfriends and girlfriends; domestic partners; neighbors; and colleagues. Inclusion of this list is intended to be illustrative only, and it is not intended to change current practices with respect to: (1) Involvement of other persons in individuals' treatment decisions; (2) informal information-sharing among individuals involved in a person's care; or (3) sharing of protected health

information to contact persons during a disaster. The final rule also includes new language stating that covered entities may use or disclose protected health information to notify or assist in notification of family members, personal representatives, or other persons responsible for an individual's care with respect to an individual's location, condition, or death. These provisions allow, for example, covered entities to notify a patient's adult child that his father has suffered a stroke and to tell the person that the father is in the hospital's intensive care unit.

The final rule includes separate provisions for situations in which the individual is present and for when the individual is not present at the time of disclosure. When the individual is present and has the capacity to make his or her own decisions, a covered entity may disclose protected health information only if the covered entity: (1) Obtains the individual's agreement to disclose to the third parties involved in their care; (2) provides the individual with an opportunity to object to such disclosure and the individual does not express an objection; or (3) reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure. Situations in which covered providers may infer an individual's agreement to disclose protected health information pursuant to option (3) include, for example, when a patient brings a spouse into the doctor's office when treatment is being discussed, and when a colleague or friend has brought the individual to the emergency room for treatment.

We proposed that when a covered entity could not practicably obtain oral agreement to disclose protected health information to next-of-kin, relatives, or those with a close personal relationship to the individual, the covered entity could make such disclosures consistent with good health professional practice and ethics. In such instances, we proposed that covered entities could disclose only the minimum information necessary for the friend or relative to provide the assistance he or she was providing. For example, health care providers could not disclose to a friend or relative simply driving a patient home from the hospital extensive information about the patient's surgery or past medical history when the friend or relative had no need for this information.

The final rule takes a similar approach. Under the final rule, when an individual is not present (for example, when a friend of a patient seeks to pick up the patient's prescription at a pharmacy) or when the opportunity to agree or object to the use or disclosure cannot practicably be provided due to the individual's incapacity or an emergency circumstance, covered entities may, in the exercise of professional judgment, determine whether the disclosure is in the individual's best interests and if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's health care. For example, this provision allows covered entities to inform relatives or others involved in a patient's care, such as the person who accompanied the individual to the emergency room, that a patient has suffered a heart attack and to provide updates on the patient's progress and prognosis when the patient is incapacitated and unable to make decisions about such disclosures. In addition, this section allows covered entities to disclose functional information to individuals assisting in a patient's care; for example, it allows hospital staff to give information about a person's mobility limitations to a friend driving the patient home from the hospital. It also allows covered entities to use professional judgment and experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on an individual's behalf to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information. Thus, under this provision, pharmacists may release a prescription to a patient's friend who is picking up the prescription for him or her. Section 164.510(b) is not intended to disrupt most covered entities' current practices or state law with respect to these types of disclosures.

This provision is intended to allow disclosures directly related to a patient's current condition and should not be construed to allow, for example, disclosure of extensive information about the patient's medical history that is not relevant to the patient's current condition and that could prove embarrassing to the patient. In addition, if a covered entity suspects that an incapacitated patient is a victim of domestic violence and that a person seeking information about the patient may have abused the patient, covered entities should not disclose information to the suspected abuser if there is reason to believe that such a disclosure could cause the patient serious harm. In all of these situations regarding possible disclosures of protected health information about an patient who is not present or is unable to agree to such disclosures due to incapacity or other emergency circumstance, disclosures should be in accordance with the exercise of professional judgment as to the patient's best interest.

This section is not intended to provide a loophole for avoiding the rule's other requirements, and it is not intended to allow disclosures to a broad range of individuals, such as journalists who may be curious about a celebrity's health status. Rather, it should be construed narrowly, to allow disclosures to those with the closest relationships with the patient, such as family members, in circumstances when a patient is unable to agree to disclosure of his or her protected health information. Furthermore, when a covered entity cannot practicably obtain an individual's agreement before disclosing protected health information to a relative or to a person involved in the individual's care and is making decisions about such disclosures consistent with the exercise of professional judgment regarding the individual's best interest, covered entities must take into account whether such a disclosure is likely to put the individual at risk of serious harm.

Like the NPRM, the final rule does not require covered entities to verify the identity of relatives or other individuals involved in the individual's care. Rather, the individual's act of involving the other persons in his or her care suffices as verification of their identity. For example, the fact that a person brings a family member into the doctor's office when treatment information will be discussed constitutes verification of the involved person's identity for purposes of this rule. Likewise, the fact that a friend arrives at a pharmacy and asks to pick up a specific prescription for an individual effectively verifies that the friend is involved in the individual's care, and the rule allows the pharmacist to give the filled prescription to the friend.

We also clarify that the final rule does not allow covered entities to assume that an individual's agreement at one point in time to disclose protected health information to a relative or to another person assisting in the individual's care implies agreement to disclose protected health information indefinitely in the future. We encourage the exercise of professional judgment in determining the scope of the person's involvement in the individual's care and the time period for which the individual is agreeing to the other person's involvement. For example, if a friend simply picks up a patient from the hospital but has played no other role

in the individual's care, hospital staff should not call the friend to disclose lab test results a month after the initial encounter with the friend. However, if a patient routinely brings a spouse into the doctor's office when treatment is discussed, a physician can infer that the spouse is playing a long-term role in the patient's care, and the rule allows disclosure of protected health information to the spouse consistent with his or her role in the patient's care, for example, discussion of treatment options.

The NPRM did not specifically address situations in which disaster relief organizations may seek to obtain protected health information from covered entities to help coordinate the individual's care, or to notify family or friends of an individual's location or general condition in a disaster situation. In the final rule, we account for disaster situations in this paragraph. Specifically, we allow covered entities to use or disclose protected health information without individual agreement to federal, state, or local government agencies engaged in disaster relief activities, as well as to private disaster relief or disaster assistance organizations (such as the Red Cross) authorized by law or by their charters to assist in disaster relief efforts, to allow these organizations to carry out their responsibilities in a specific disaster situation. Covered entities may make these disclosures to disaster relief organizations, for example, so that these organizations can help family members, friends, or others involved in the individual's care to locate individuals affected by a disaster and to inform them of the individual's general health condition. This provision also allows disclosure of information to disaster relief or disaster assistance organizations so that these organizations can help individuals obtain needed medical care for injuries or other health conditions caused by a disaster.

We encourage disaster relief organizations to protect the privacy of individual health information to the extent practicable in a disaster situation. However, we recognize that the nature of disaster situations often makes it impossible or impracticable for disaster relief organizations and covered entities to seek individual agreement or authorization before disclosing protected health information necessary for providing disaster relief. Thus, we note that we do not intend to impede disaster relief organizations in their critical mission to save lives and reunite loved ones and friends in disaster situations.

Section 164.512—Uses and Disclosures for Which Consent, an Authorization, or Opportunity To Agree or Object Is Not Required

Introduction

The final rule's requirements regarding disclosures for directory information and to family members or others involved in an individual's care are in a section separate from that covering disclosures allowed for other national priority purposes. In the final rule, we place most of the other disclosures for national priority purposes in a new § 164.512.

As in the NPRM, in § 164.512 of the final rule, we allow covered entities to make these national priority uses and disclosures without individual authorization. As in the NPRM, these uses and disclosures are discretionary. Covered entities are free to decide whether or not to use or disclose protected health information for any or all of the permitted categories. However, as in the NPRM, nothing in the final rule provides authority for a covered entity to restrict or refuse to make a use or disclosure mandated by other law.

The new § 164.512 includes paragraphs on: Uses and disclosures required by law; uses and disclosures for public health activities; disclosures about victims of abuse, neglect, or domestic violence; uses and disclosures for health oversight activities; disclosures for judicial and administrative proceedings; disclosures for law enforcement purposes; uses and disclosures about decedents; uses and disclosures for cadaveric donation of organs, eyes, or tissues; uses and disclosures for research purposes; uses and disclosures to avert a serious threat to health or safety (which we had called ''emergency circumstances'' in the NPRM); uses and disclosures for specialized government functions (referred to as ''specialized classes'' in the NPRM); and disclosures to comply with workers' compensation laws.

Section 164.512(c) in the final rule, which addresses uses and disclosures regarding adult victims of abuse, neglect and domestic violence, is new, although it incorporates some provisions from proposed § 164.510 of the NPRM. In the final rule we also eliminate proposed § 164.510(g) on government health data systems and proposed § 164.510(i) on banking and payment processes. These changes are discussed below.

Approach to Use of Protected Health Information

Proposed § 164.510 of the NPRM included specific subparagraphs addressing uses of protected health information by covered entities that were also public health agencies, health oversight agencies, government entities conducting judicial or administrative proceedings, or government heath data systems. Such covered entities could use protected health information in all instances for which they could disclose the information for these purposes. In the final rule, as discussed below, we retain this language in the paragraphs on public health activities and health oversight. However, we eliminate this clause with respect to uses of protected health information for judicial and administrative proceedings, because we no longer believe that there would be any situations in which a covered entity would also be a judicial or administrative tribunal. Proposed § 164.510(e) of the NPRM, regarding disclosure of protected health information to coroners, did not include such a provision. In the final rule we have added it because we believe there are situations in which a covered entity, for example, a public hospital conducting post-mortem investigations, may need to use protected health information for the same purposes for which it would have disclosed the information to a coroner.

While the right to request restrictions under § 164.522 and the consents required under § 164.506 do not apply to the use and disclosure of protected health information under § 164.512, we do not intend to preempt any state or other restrictions, or any right to enforce such agreements or consents under other law.

We note that a covered entity may use or disclose protected health information as permitted by and in accordance with one of the paragraphs of § 164.512, regardless of whether that use or disclosure fails to meet the requirements for use or disclosure under a different paragraph in § 164.512 or elsewhere in the rule.

Verification for Disclosures Under § 164.512

In § 164.510(a) of the NPRM, we proposed that covered entities verify the identity and authority of persons to whom they made disclosure under the section. In the final rule, we generally have retained the proposed requirements. Verification requirements are discussed in § 164.514 of the final rule.

Section 164.512(a)—Uses and Disclosures Required by Law

In the NPRM we would have allowed covered entities to use or disclose protected health information without individual authorization where such use

or disclosure was required by other law, as long as the use or disclosure met all relevant requirements of such law. However, a legally mandated use or disclosure which fell into one or more of the national priority purposes expressly identified in proposed § 164.510 of the NPRM would have been subject to the terms and conditions specified by the applicable paragraph of proposed § 164.510. Thus, a disclosure required by law would have been allowed only to the extent it was not otherwise prohibited or restricted by another provision in proposed § 164.510. For example, mandatory reporting to law enforcement officials would not have been allowed unless such disclosures conformed to the requirements of proposed § 164.510(f) of the NPRM, on uses and disclosures for law enforcement purposes. As explained in the NPRM, this provision was not intended to obstruct access to information deemed important enough by federal, state or other government authorities to require it by law.

In § 164.512(a) of the final rule, we retain the proposed approach, and we permit covered entities to comply with laws requiring the use or disclosure of protected health information, provided the use or disclosure meets and is limited to the relevant requirements of such other laws. To more clearly address where the substantive and procedural requirements of other provisions in this section apply, we have deleted the general sentence from the NPRM which stated that the provision ''does not apply to uses or disclosures that are covered by paragraphs (b) through (m)'' of proposed § 164.510. Instead, in § 164.512 (a)(2) we list the specific paragraphs that have additional requirements with which covered entities must comply. They are disclosures about victims of abuse, neglect or domestic violence (§ 164.512(c)), for judicial and administrative proceedings (§ 164.512(e)), and for law enforcement purposes (§ 164.512(f)). We include a new definition of ''required by law.'' See § 164.501. We clarify that the requirements provided for in § 164.514(h) relating to verification apply to disclosures under this paragraph. Those provisions require covered entities to verify the identity and authority of persons to whom they make disclosures. We note that the minimum necessary requirements of § 164.514(d) do not apply to disclosures made under this paragraph.

We note that this rule does not affect what is required by other law, nor does it compel a covered entity to make a use or disclosure of protected health information required by the legal demands or reporting requirements listed in the definition of ''required by law.'' Covered entities will not be sanctioned under this rule for responding in good faith to such legal process and reporting requirements. However, nothing in this rule affects, either by expanding or contracting, a covered entity's right to challenge such process or reporting requirements under other laws. The only disclosures of protected health information compelled by this rule are disclosures to an individual (or the personal representative of an individual) or to the Secretary for the purposes of enforcing this rule.

Uses and disclosures permitted under this paragraph must be limited to the protected health information necessary to meet the requirements of the law that compels the use or disclosure. For example, disclosures pursuant to an administrative subpoena are limited to the protected health information authorized to be disclosed on the face of the subpoena.

Section 164.512(b)—Uses and Disclosures for Public Health Activities

The NPRM would have allowed covered entities to disclose protected health information without individual authorization to: (1) A public health authority authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; (2) a public health authority or other appropriate authority authorized by law to receive reports of child abuse or neglect; (3) a person or entity other than a governmental authority that could demonstrate or demonstrated that it was acting to comply with requirements or direction of a public health authority; or (4) a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition and was authorized by law to be notified as necessary in the conduct of a public health intervention or investigation.

In the final rule, we broaden the scope of permissible disclosures pursuant to item (1) listed above. We narrow the scope of disclosures permissible under item (3) of this list, and we add language to clarify the scope of permissible disclosures with respect to item (4) on the list. We broaden the scope of allowable disclosures regarding item (1) by allowing covered entities to disclose protected health information not only to U.S. public health authorities but also, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority. For example, we allow covered entities to disclose protected health information to a foreign government agency that is collaborating with the Centers for Disease Control and Prevention to limit the spread of infectious disease.

We narrow the conditions under which covered entities may disclose protected health information to non-government entities. We allow covered entities to disclose protected health information to a person subject to the FDA's jurisdiction, for the following activities: to report adverse events (or similar reports with respect to food or dietary supplements), product defects or problems, or biological product deviations, if the disclosure is made to the person required or directed to report such information to the FDA; to track products if the disclosure is made to a person required or directed by the FDA to track the product; to enable product recalls, repairs, or replacement, including locating and notifying individuals who have received products regarding product recalls, withdrawals, or other problems; or to conduct post-marketing surveillance to comply with requirements or at the direction of the FDA.

The terms included in § 164.512(b)(iii) are intended to have both their commonly understood meanings, as well as any specialized meanings, pursuant to the Food, Drug, and Cosmetic Act (21 U.S.C. 321 *et seq.*) or the Public Health Service Act (42 U.S.C. 201 *et seq.*). For example, ''post-marketing surveillance'' is intended to mean activities related to determining the safety or effectiveness of a product after it has been approved and is in commercial distribution, as well as certain Phase IV (post-approval) commitments by pharmaceutical companies. With respect to devices, ''post-marketing surveillance'' can be construed to refer to requirements of section 522 of the Food, Drug, and Cosmetic Act regarding certain implanted, life-sustaining, or life-supporting devices. The term ''track'' includes, for example, tracking devices under section 519(e) of the Food, Drug, and Cosmetic Act, units of blood or other blood products, as well as trace-backs of contaminated food.

In § 164.512(b)(iii), the term ''required'' refers to requirements in statute, regulation, order, or other

legally binding authority exercised by the FDA. The term ''directed,'' as used in this section, includes other official agency communications such as guidance documents.

We note that under this provision, a covered entity may disclose protected health information to a non-governmental organization without individual authorization for inclusion in a private data base or registry only if the disclosure is otherwise for one of the purposes described in this provision (*e.g.,* for tracking products pursuant to FDA direction or requirements, for post-marketing surveillance to comply with FDA requirements or direction.)

To make a disclosure that is not for one of these activities, covered entities must obtain individual authorization or must meet the requirements of another provision of this rule. For example, covered entities may disclose protected health information to employers for inclusion in a workplace surveillance database only: with individual authorization; if the disclosure is required by law; if the disclosure meets the requirements of § 164.512(b)(v); or if the disclosure meets the conditions of another provision of this regulation, such as § 154.512(i) relating to research. Similarly, if a pharmaceutical company seeks to create a registry containing protected health information about individuals who had taken a drug that the pharmaceutical company had developed, covered entities may disclose protected health information without authorization to the pharmaceutical company pursuant to FDA requirements or direction. If the pharmaceutical company's registry is not for any of these purposes, covered entities may disclose protected health information to it only with patient authorization, if required by law, or if disclosure meets the conditions of another provision of this rule.

The final rule continues to permit covered entities to disclose protected health information without individual authorization directly to public health authorities, such as the Food and Drug Administration, the Occupational Safety and Health Administration, the Centers for Disease Control and Prevention, as well as state and local public health departments, for public health purposes as specified in the NPRM.

The final rule retains the NPRM provision allowing covered entities to disclose protected health information to public health authorities or other appropriate government authorities authorized by law to receive reports of child abuse or neglect. In addition, we clarify the NPRM's provision regarding disclosure of protected health information to persons who may have been exposed to a communicable disease or who may otherwise be at risk of contracting or spreading a disease or condition. Under the final rule, covered entities may disclose protected health information to such individuals when the covered entity or public health authority is authorized by law to notify these individuals as necessary in the conduct of a public health intervention or investigation.

In addition, as in the NPRM, under the final rule, a covered entity that is acting as a public health authority—for example, a public hospital conducting infectious disease surveillance in its role as an arm of the public health department—may use protected health information in all cases for which it is allowed to disclose such information for public health activities as described above.

The proposed rule did not contain a specific provision relating to disclosures by covered health care providers to employers concerning work-related injuries or illnesses or workplace medical surveillance. Under the proposed rule, a covered entity would have been permitted to disclose protected health information without individual authorization for public health purposes to private person if the person could demonstrate that it was acting to comply with requirements or at the direction of a public health authority.

As discussed above, in the final rule we narrow the scope of this paragraph as it applies to disclosures to persons other than public health authorities. To ensure that covered health care providers may make disclosures of protected health information without individual authorization to employers when appropriate under federal and state laws addressing work-related injuries and illnesses or workplace medical surveillance, we include a new provision in the final rule. The provision permits covered health care providers who provide health care as a workforce member of or at the request of an employer to disclose to that employer protected health information concerning work-related injuries or illnesses or workplace medical surveillance in situations where the employer has a duty under the Occupational Safety and Health Act, the Federal Mine Safety and Health Act, or under a similar state law, to keep records on or act on such information. For example, OSHA regulations in 29 CFR part 1904 require employers to record work-related injuries and illnesses if medical treatment is necessary; MSHA regulations at 30 CFR part 50 require mine operators to report injuries and illnesses experienced by miners. Similarly, OSHA rules require employers to monitor employees' exposure to certain substances and to remove employees from exposure when toxic thresholds have been met. To obtain the relevant health information necessary to determine whether an injury or illness should be recorded, or whether an employee must be medically removed from exposure at work, employers must refer employees to health care providers for examination and testing.

OSHA and MSHA rules do not impose duties directly upon health care providers to disclose health information pertaining to recordkeeping and medical monitoring requirements to employers. Rather, these rules operate on the presumption that health care providers who provide services at the request of an employer will be able to disclose to the employer work-related health information necessary for the employer to fulfill its compliance obligations. This new provision permits covered entities to make disclosures necessary for the effective functioning of OSHA and MSHA requirements, or those of similar state laws, by permitting a health care provider to make disclosures without the authorization of the individual concerning work-related injuries or illnesses or workplace medical surveillance in situations where the employer has a duty under OSHA and MSHA requirements, or under a similar state laws, to keep records on or act on such information.

We require health care providers who make disclosures to employers under this provision to provide notice to individuals that it discloses protected health information to employers relating to the medical surveillance of the workplace and work-related illnesses and injuries. The notice required under this provision is separate from the notice required under § 164.520. The notice required under this provision may be met giving a copy of the notice to the individual at the time it provides the health care services, or, if the health care services are provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care services are provided.

This provision applies only when a covered health care provider provides health care services as a workforce member of or at the request of an employer and for the purposes discussed above. The provision does not affect the application of this rule to other health care provided to

individuals or to their relationship with health care providers that they select.

Section 164.512(c)—Disclosures About Victims of Abuse, Neglect or Domestic Violence

The NPRM included two provisions related to disclosures about persons who are victims of abuse. In the NPRM, we would have allowed covered entities to report child abuse to a public health authority or other appropriate authority authorized by law to receive reports of child abuse or neglect. In addition, under proposed § 164.510(f)(3) of the NPRM, we would have allowed covered entities to disclose protected health information about a victim of a crime, abuse or other harm to a law enforcement official under certain circumstances. The NPRM recognized that most, if not all, states had laws that mandated reporting of child abuse or neglect to the appropriate authorities. Moreover, HIPAA expressly carved out state laws on child abuse and neglect from preemption or any other interference. The NPRM further acknowledged that most, but not all, states had laws mandating the reporting of abuse, neglect or exploitation of the elderly or other vulnerable adults. We did not intend to impede reporting in compliance with these laws.

The final rule includes a new paragraph, § 164.512(c), which allows covered entities to report protected health information to specified authorities in abuse situations other than those involving child abuse and neglect. In the final rule, disclosures of protected health information related to child abuse continues to be addressed in the paragraph allowing disclosure for public health activities (§ 164.512(b)), as described above. Because HIPAA addresses child abuse specifically in connection with a state's public health activities, we believe it would not be appropriate to include child abuse-related disclosures in this separate paragraph on abuse. State laws continue to apply with respect to child abuse, and the final rule does not in any way interfere with a covered entity's ability to comply with these laws.

In the final rule, we address disclosures about other victims of abuse, neglect and domestic violence in § 164.512(c) rather than in the law enforcement paragraph. Section 164.512(c) establishes conditions for disclosure of protected health information in cases involving domestic violence other than child abuse (*e.g.,* spousal abuse), as well as those involving abuse or neglect (*e.g.,* abuse of nursing home residents or residents of facilities for the mentally retarded). This paragraph addresses reports to law enforcement as well as to other authorized public officials. The provisions of this paragraph supersede the provisions of § 164.512(a) and § 164.512(f)(1)(i) to the extent that those provisions address the subject matter of this paragraph.

Under the circumstances described below, the final rule allows covered entities to disclose protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence. In this paragraph, references to ''individual'' should be construed to mean the individual believed to be the victim. The rule allows such disclosure to any governmental authority authorized by law to receive reports of such abuse, neglect, or domestic violence. These entities may include, for example, adult protective or social services agencies, state survey and certification agencies, ombudsmen for the aging or those in long-term care facilities, and law enforcement or oversight.

The final rule specifies three circumstances in which disclosures of protected health information is allowed in order to report abuse, neglect or domestic violence. First, this paragraph allows disclosure of protected health information related to abuse if required by law and the disclosure complies with and is limited to the relevant requirements of such law. As discussed below, the final rule requires covered entities that make such disclosures pursuant to a state's mandatory reporting law to inform the individual of the report.

Second, this paragraph allows covered entities to disclose protected health information related to abuse if the individual has agrees to such disclosure. When considering the possibility of disclosing protected health information in an abuse situation pursuant to this section, we encourage covered entities to seek the individual's agreement whenever possible.

Third, this paragraph allows covered entities to disclose protected health information about an individual without the individual's agreement if the disclosure is expressly authorized by statute or regulation and either: (1) The covered entity, in the exercise of its professional judgment, believes that the disclosure is necessary to prevent serious harm to the individual or to other potential victims; or (2) if the individual is unable to agree due to incapacity, a law enforcement or other public official authorized to received the report represents that the protected health information for which disclosure is sought is not intended to be used against the individual, and that an immediate enforcement activity that depends on the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

We emphasize that disclosure under this third part of the paragraph also may be made only if it is expressly authorized by statute or regulation. We use this formulation, rather than the broader ''required by law,'' because of the heightened privacy and safety concerns in these situations. We believe it appropriate to defer to other public determinations regarding reporting of this information only where a legislative or executive body has determined the reporting to be of sufficient importance to warrant enactment of a law or promulgation of a regulation. Law and regulations reflect a clear decision to authorize the particular disclosure of protected health information, and reflect greater public accountability (*e.g.,* through the required public comment process or because enacted by elected representatives).

For example, a Wisconsin law (Wis. Stat § 46.90(4)) states that any person may report to a county agency or state official that he or she believes that abuse or neglect has occurred. Pursuant to § 164.512(c)(1)(iii), a covered entity may make a report only if the specific type or subject matter of the report (*e.g.,* abuse or neglect of the elderly) is included in the law authorizing the report, and such a disclosure may only be made to a public authority specifically identified in the law authorizing the report. Furthermore, we note that disclosures under this part of the paragraph are further limited to two circumstances. In the first case, a covered entity, in the exercise of professional judgment, must believe that the disclosure is necessary to prevent serious harm to the individual or to other potential victims. The second case addresses situations in which an individual who is a victim of abuse, neglect or domestic violence is unable to agree due to incapacity and a law enforcement or other public official authorized to receive the report represents that the protected health information for which disclosure is sought is not intended to be used against the individual and that an immediate law enforcement activity that depends on the disclosure would be materially and adversely affected by waiting until the individual if able to agree to the disclosure. We note that, in this second case, a covered entity may exercise discretion, consistent with professional judgment as to the patient's

best interest, in deciding whether to make the requested disclosure.

The rules governing disclosure in this third set of circumstances are different from those governing disclosures pursuant to § 164.512(f)(3) regarding disclosure to law enforcement about victims of crime and other harm. We believe that in abuse situations—to a greater extent than in situations involving crime victims in general—there is clear potential for abusers to cause further serious harm to the victim or to others, such as other family members in a household or other residents of a nursing home. The provisions allowing reporting of abuse when authorized by state law, as described above, are consistent with principles articulated by the AMA's Council on Ethical and Judicial Affairs, which state that when reporting abuse is voluntary under state law, it is justified when necessary to prevent serious harm to a patient. Through the provisions of § 164.512(c), we recognize the unique circumstances surrounding abuse and domestic violence, and we seek to provide an appropriate balance between individual privacy interests and important societal interests such as preventing serious harm to other individuals. We note that here we are relying on covered entities, in the exercise of professional judgment, to determine what is in the best interests of the patient.

Finally, we require covered entities to inform the individual in all of the situations described above that the covered entity has disclosed protected health information to report abuse, neglect, or domestic violence. We allow covered entities to provide this information orally. We do not require written notification, nor do we encourage it, due to the sensitivity of abuse situations and the potential for the abuser to cause further harm to the individual if, for example, a covered entity sends written notification to the home of the individual and the abuser. Whenever possible, covered entities should inform the individual at the same time that they determine abuse has occurred and decide that the abuse should be reported. In cases involving patient incapacity, we encourage covered entities to inform the individual of such disclosures as soon as it is practicable to do so.

The rule provides two exceptions to the requirement to inform the victim about a report to a government authority, one based on concern for future harm and one based on past harm. First, a covered entity need not inform the victim if the covered entity, in the exercise of professional judgment, believes that informing the individual would place the individual at risk of serious harm. We believe that this exception is necessary to address the potential for future harm, either physical or emotional, that the individual may face from knowing that the report has been made. Second, a covered entity may choose not to meet the requirement for informing the victim, if the covered entity actually would be informing a personal representative (such as a parent of a minor) and the covered entity reasonably believes that such person is responsible for the abuse, neglect, or other injury that has already occurred and that informing that person would not be in the individual's best interests.

Section 164.512(d)—Uses and Disclosures for Health Oversight Activities

Under § 164.510(c) of the NPRM, we proposed to permit covered entities to disclose protected health information to health oversight agencies for oversight activities authorized by law, including audit, investigation, inspection, civil, criminal, or administrative proceeding or action, or other activity necessary for appropriate oversight of: (i) the health care system; (ii) government benefit programs for which health information is relevant to beneficiary eligibility; or (iii) government regulatory programs for which health information is necessary for determining compliance with program standards.

In § 164.512(d) of the final rule, we modify the proposed language to include civil and criminal investigations. In describing ''other activities necessary for oversight'' of particular entities, we add the phrase ''entities subject to civil rights laws for which health information is necessary for determining compliance.'' In addition, in the final rule, we add ''licensure or disciplinary actions'' to the list of oversight activities authorized by law for which covered entities may disclose protected health information to health oversight agencies. The NPRM's definition of ''health oversight agency'' (in proposed § 164.504) included this phrase, but it was inadvertently excluded from the regulation text at proposed § 164.510(c). We make this change in the regulation text of the final rule to conform to the NPRM's definition of health oversight agency and to reflect the full range of activities for which we intend to allow covered entities to disclose protected health information to health oversight agencies.

The NPRM would have allowed, but would not have required, covered entities to disclose protected health information to public oversight agencies and to private entities acting under grant of authority from or under contract with oversight agencies for oversight purposes without individual authorization for health oversight activities authorized by law. When a covered entity was also an oversight agency, it also would have been permitted to use protected health information in all cases in which it would have been allowed to disclose such information for health oversight purposes. The NPRM would not have established any new administrative or judicial process prior to disclosure for health oversight, nor would it have permitted disclosures forbidden by other law. The proposed rule also would not have created any new right of access to health records by oversight agencies, and it could not have been used as authority to obtain records not otherwise legally available to the oversight agency.

The final rule retains this approach to health oversight. As in the NPRM, the final rule provides that when a covered entity is also an oversight agency, it is allowed to use protected health information in all cases in which it is allowed to disclose such information for health oversight purposes. For example, if a state insurance department is acting as a health plan in operating the state's Medicaid managed care program, the final rule allows the insurance department to use protected health information in all cases for which the plan can disclose the protected health information for health oversight purposes. For example, the state insurance department in its capacity as the state Medicaid managed care plan can use protected health information in the process of investigating and disciplining a state Medicaid provider for attempting to defraud the Medicaid system. As in the NPRM, the final rule does not establish any new administrative or judicial process prior to disclosure for health oversight, nor does it prohibit covered entities from making any disclosures for health oversight that are otherwise required by law. Like the NPRM, it does not create any new right of access to health records by oversight agencies and it cannot be used as authority to obtain records not otherwise legally available to the oversight agency.

Overlap Between Law Enforcement and Oversight

Under the NPRM, the proposed definitions of law enforcement and oversight, and the rules governing disclosures for these purposes

overlapped. Specifically, this overlap occurred because: (1) The NPRM preamble, but not the NPRM regulation text, indicated that agencies conducting both oversight and law enforcement activities would be subject to the oversight requirements when conducting oversight activities; and (2) the NPRM addressed some disclosures for investigations of health care fraud in the law enforcement paragraph (proposed § 164.510(f)(5)(i)), while health care fraud investigations are central to the purpose of health care oversight agencies (covered under proposed § 164.510(c)). In the final rule, we make substantial changes to these provisions, in an attempt to prevent confusion.

In § 164.512(d)(2), we include explicit decision rules indicating when an investigation is considered law enforcement and when an investigation is considered oversight under this regulation. An investigation or activity is not considered health oversight for purposes of this rule if: (1) The individual is the subject of the investigation or activity; and (2) The investigation or activity does not arise out of and is not directly related to: (a) The receipt of health care; (b) a claim for public benefits related to health; or (c) qualification for, or receipt of public benefits or services where a patient's health is integral to the claim for benefits or services. In such cases, where the individual is the subject of the investigation and the investigation does not relate to issues (a) through (c), the rules regarding disclosure for law enforcement purposes (see § 164.512(f)) apply. For the purposes of this rule, we intend for investigations regarding issues (a) through (c) above to mean investigations of health care fraud.

Where the individual is not the subject of the activity or investigation, or where the investigation or activity relates to the subject matter in (a) through (c) of the preceding sentence, a covered entity may make a disclosure pursuant to § 164.512(d)(1). For example, when the U.S. Department of Labor's Pension and Welfare Benefits Administration (PWBA) needs to analyze protected health information about health plan enrollees in order to conduct an audit or investigation of the health plan (*i.e.,* the enrollees are not subjects of the investigation) to investigate potential fraud by the plan, the health plan may disclose protected health information to the PWBA under the health oversight rules. These rules and distinctions are discussed in greater detail in our responses to comments.

To clarify further that health oversight disclosure rules apply generally in health care fraud investigations (subject to the exception described above), in the final rule, we eliminate proposed § 164.510(f)(5)(i), which would have established requirements for disclosure related to health care fraud for law enforcement purposes. All disclosures of protected health information that would have been permitted under proposed § 164.510(f)(5)(i) are permitted under § 164.512(d).

In the final rule, we add new language (§ 164.512(d)(3)) to address situations in which health oversight activities are conducted in conjunction with an investigation regarding a claim for public benefits not related to health (*e.g.,* claims for Food Stamps). In such situations, for example, when a state Medicaid agency is working with the Food Stamps program to investigate suspected fraud involving Medicaid and Food Stamps, covered entities may disclose protected health information to the entities conducting the joint investigation under the health oversight provisions of the rule.

In the proposed rule, the definitions of ''law enforcement proceeding'' and ''oversight activity'' both included the phrase ''criminal, civil, or administrative proceeding.'' For reasons explained below, the final rule retains this phrase in both definitions. The final rule does not attempt to distinguish between these activities based on the agency undertaking them or the applicable enforcement procedures. Rather, as described above, the final rule carves out certain activities which must always be considered law enforcement for purposes of disclosure of protected health information under this rule.

Additional Considerations

We note that covered entities are permitted to initiate disclosures that are permitted under this paragraph. For example, a covered entity could disclose protected health information in the course of reporting suspected health care fraud to a health oversight agency.

We delete language in the NPRM that would have allowed disclosure under this section only to law enforcement officials conducting or supervising an investigation, official inquiry, or a criminal, civil or administrative proceeding authorized by law. In some instances, a disclosure by a covered entity under this section will initiate such an investigation or proceeding, but it will not already be ongoing at the time the disclosure is made.

Section 164.512(e)—Disclosures and Uses for Judicial and Administrative Proceedings

Section 164.512(e) addresses when a covered entity is permitted to disclose protected health information in response to requests for protected health information that are made in the course of judicial and administrative proceedings—for example, when a non-party health care provider receives a subpoena (under Federal Rule of Civil Procedure Rule 45 or similar provision) for medical records from a party to a law suit. In the NPRM we would have allowed covered entities to disclose protected health information in the course of any judicial or administrative proceeding: (1) In response to an order of a court or administrative tribunal; or (2) where an individual was a party to the proceeding and his or her medical condition or history was at issue and the disclosure was pursuant to lawful process or otherwise authorized by law. Under the NPRM, if the request for disclosure of protected health information was accompanied by a court order, a covered entity could have disclosed that protected health information which the court order authorized to be disclosed. If the request for disclosure of protected health information were not accompanied by a court order, covered entities could not have disclosed the information requested unless a request authorized by law had been made by the agency requesting the information or by legal counsel representing a party to litigation, with a written statement certifying that the protected health information requested concerned a litigant to the proceeding and that the health condition of the litigant was at issue at the proceeding.

In § 164.512(e) of the final rule, we permit covered entities to disclose protected health information in a judicial or administrative proceeding if the request for such protected health information is made through or pursuant to an order from a court or administrative tribunal or in response to a subpoena or discovery request from, or other lawful process by a party to the proceeding. When a request is made pursuant to an order from a court or administrative tribunal, a covered entity may disclose the information requested without additional process. For example, a subpoena issued by a court constitutes a disclosure which is required by law as defined in this rule, and nothing in this rule is intended to interfere with the ability of the covered entity to comply with such subpoena.

However, absent an order of, or a subpoena issued by, a court or administrative tribunal, a covered entity may respond to a subpoena or discovery request from, or other lawful process by, a party to the proceeding only if the covered entity obtains either: (1) Satisfactory assurances that reasonable efforts have been made to give the individual whose information has been requested notice of the request; or (2) satisfactory assurances that the party seeking such information has made reasonable efforts to secure a protective order that will guard the confidentiality of the information. In meeting the first test, a covered entity is considered to have received satisfactory assurances from the party seeking the information if that party demonstrates that it has made a good faith effort (such as by sending a notice to the individual's last known address) to provide written notice to the individual whose information is the subject of the request, that the written notice included sufficient information about the proceeding to permit the individual to raise an objection, and that the time for the individual to raise objections to the court or administrative tribunal has elapsed and no objections were filed or any objections filed by the individual have been resolved.

Unless required to do so by other law, the covered entity is not required to explain the procedures (if any) available for the individual to object to the disclosure. Under the rule, the individual exercises the right to object before the court or other body having jurisdiction over the proceeding, and not to the covered entity. The provisions in this paragraph are not intended to disrupt current practice whereby an individual who is a party to a proceeding and has put his or her medical condition at issue will not prevail without consenting to the production of his or her protected health information. In such cases, we presume that parties will have ample notice and an opportunity to object in the context of the proceeding in which the individual is a party.

As described above, in this paragraph we also permit a covered entity to disclose protected health information in response to a subpoena, discovery request, or other lawful process if the covered entity receives satisfactory assurances that the party seeking the information has made reasonable efforts to seek a qualified protective order that would protect the privacy of the information. A ''qualified protective order'' means an order of a court or of an administrative tribunal or a stipulation that: (1) Prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which the records are requested; and (2) requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding. Satisfactory assurances of reasonable efforts to secure a qualified protective order are a statement and documentation that the parties to the dispute have agreed to a protective order and that it has been submitted to the court or administrative tribunal with jurisdiction, or that the party seeking the protected health information has requested a qualified protective order from such court or tribunal. We encourage the development of ''model'' protective orders that will facilitate adherence with this subpart.

In the final rule we also permit the covered entity itself to satisfy the requirement to make reasonable efforts to notify the individual whose information has been requested or to seek a qualified protective order. We intend this to be a permissible activity for covered entities: we do not require covered entities to undertake these efforts in response to a subpoena, discovery request, or similar process (other than an order from a court or administrative tribunal). If a covered entity receives such a request without receiving the satisfactory assurances described above from the party requesting the information, the covered entity is free to object to the disclosure and is not required to undertake the reasonable efforts itself.

We clarify that the provisions of this paragraph do not supersede or otherwise invalidate other provisions of this rule that permit uses and disclosures of protected health information. For example, the fact that protected health information is the subject of a matter before a court or tribunal does not prevent its disclosure under another provision of the rule, such as §§ 164.512(b), 164.512(d), or 164.512(f), even if a public agency's method of requesting the information is pursuant to an administrative proceeding. For example, where a public agency commences a disciplinary action against a health professional, and requests protected health information as part of its investigation, the disclosure made be made to the agency under paragraph (d) of this section (relating to health oversight) even if the method of making the request is through the proceeding. As with any request for disclosure under this section, the covered entity will need to verify the authority under which the request is being made, and we expect that public agencies will identify their authority when making such requests. We note that covered entities may reasonably rely on assertions of authority made by government agencies.

Additional Considerations

Where a disclosure made pursuant to this paragraph is required by law, such as in the case of an order from a court or administrative tribunal, the minimum necessary requirements in § 164.514(d) do not apply to disclosures made under this paragraph. A covered entity making a disclosure under this paragraph, however, may of course disclose only that protected health information that is within the scope of the permitted disclosure. For instance, in response to an order of a court or administrative tribunal, the covered entity may disclose only the protected health information that is expressly authorized by such an order. Where a disclosure is not considered under this rule to be required by law, the minimum necessary requirements apply, and the covered entity must make reasonable efforts to limit the information disclosed to that which is reasonably necessary to fulfill the request. A covered entity is not required to second guess the scope or purpose of the request, or take action to resist the request because they believe that it is over broad. In complying with the request, however, the covered entity must make reasonable efforts not to disclose more information than is requested. For example, a covered entity may not provide a party free access to its medical records under the theory that the party can identify the information necessary for the request. In some instances, it may be appropriate for a covered entity, presented with a relatively broad discovery request, to permit access to a relatively large amount of information in order for a party to identify the relevant information. This is permissible as long as the covered entity makes reasonable efforts to circumscribe the access as appropriate.

The NPRM indicated that when a covered entity was itself a government agency, the covered entity could use protected health information in all cases in which it would have been allowed to disclose such information in the course of any judicial or administrative proceeding. As explained above, the final rule does not include this provision.

Section 164.512(f)—Disclosure for Law Enforcement Purposes

Disclosures Pursuant to Process and as Otherwise Required by Law

In the NPRM we would have allowed covered entities to disclose protected health information without individual authorization as required by other law. However, as explained above, if a legally mandated use or disclosure fell into one or more of the national priority purposes expressly identified in other paragraphs of proposed § 164.510, the disclosure would have been subject to the terms and conditions specified by the applicable paragraph of proposed § 164.510. For example, mandatory reporting to law enforcement officials would not have been allowed unless such disclosures conformed to the requirements of proposed § 164.510(f) of the NPRM. Proposed § 164.510(f) did not explicitly recognize disclosures required by other laws, and it would not have permitted covered entities to comply with some state and other mandatory reporting laws that require covered entities to disclose protected health information to law enforcement officials, such as the reporting of gun shot wounds, stab wounds, and/or burn injuries.

We did not intend to preempt generally state and other mandatory reporting laws, and in § 164.512(f)(1)(i) of the final rule, we explicitly permit covered entities to disclose protected health information for law enforcement purposes as required by other law. This provision permits covered entities to comply with these state and other laws. Under this provision, to the extent that a mandatory reporting law falls under the provisions of § 164.512(c)(1)(i) regarding reporting of abuse, neglect, or domestic violence, the requirements of those provisions supersede.

In the final rule, we specify that covered entities may disclose protected health information pursuant to this provision in compliance with and as limited by the relevant requirements of legal process or other law. In the NPRM, for the purposes of this portion of the law enforcement paragraph, we proposed to define ''law enforcement inquiry or proceeding'' as an investigation or official proceeding inquiring into a violation of or failure to comply with law; or a criminal, civil or administrative proceeding arising from a violation of or failure to comply with law. In the final rule, we do not include this definition in § 164.512(f), because it is redundant with the definition of ''law enforcement official'' in § 164.501.

Proposed § 164.510(f)(1) of the NPRM would have authorized disclosure of protected health information to a law enforcement official conducting or supervising a law enforcement inquiry or proceeding authorized by law pursuant to process, under three circumstances.

First, we proposed to permit such disclosures pursuant to a warrant, subpoena, or other order issued by a judicial officer that documented a finding by the officer. The NPRM did not specify requirements for the nature of the finding. In the final rule, we eliminate the requirement for a ''finding,'' and we make changes to the list of orders in response to which covered entities may disclose under this provision. Under the final rule, covered entities may disclose protected health information in compliance with and as limited by relevant requirements of: a court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer. We made this change to the list to conform to the definition of ''required by law'' in § 164.501.

Second, we proposed to permit such disclosures pursuant to a state or federal grand jury subpoena. In the final rule, we leave this provision of the NPRM unchanged.

Third, we proposed to permit such disclosures pursuant to an administrative request, including an administrative subpoena or summons, a civil investigative demand, or similar process, under somewhat stricter standards than exist today for such disclosures. We proposed to permit a covered entity to disclose protected health information pursuant to an administrative request only if the request met three conditions, as follows: (i) The information sought was relevant and material to a legitimate law enforcement inquiry; (ii) the request was as specific and narrowly drawn as reasonably practicable; and (iii) de-identified information could not reasonably have been used to meet the purpose of the request.

The final rules generally adopts this provision of the NPRM. In the final rule, we modify the list of orders in response to which covered entities may disclose protected health information, to include administrative subpoenas or summons, civil or authorized investigative demands, or similar process authorized by law. We made this change to the list to conform with the definition of ''required by law'' in § 164.501. In addition, we slightly modify the second of the three conditions under which covered entities may respond to such requests, to allow disclosure if the request is specific and is limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.

Limited Information for Identification and Location Purposes

The NPRM would have allowed covered entities to disclose ''limited identifying information'' for purposes of identifying a suspect, fugitive, material witness, or missing person, in response to a law enforcement request. We proposed to define ''limited identifying information'' as (i) name; (ii) address; (iii) Social Security number; (iv) date of birth; (v) place of birth; (vi) type of injury or other distinguishing characteristic; and (vii) date and time of treatment.

The final rules generally adopts this provision of the NPRM with a few modifications. In the final rule, we expand the circumstances under which limited information about suspects, fugitives, material witnesses, and missing persons may be disclosed, to include not only cases in which law enforcement officials are seeking to identify such individuals, but also cases in which law enforcement officials are seeking to locate such individuals. In addition, the final rule modifies the list of data elements that may be disclosed under this provision, in several ways. We expand the list of elements that may be disclosed under these circumstances, to include ABO blood type and Rh factor, as well as date and time of death, if applicable. We remove ''other distinguishing characteristic'' from the list of items that may be disclosed for the location and identification purposes described in this paragraph, and instead allow covered entities to disclose only a description of distinguishing physical characteristics, such as scars and tattoos, height, weight, gender, race, hair and eye color, and the presence or absence of facial hair such as a beard or moustache. In addition, in the final rule, protected health information associated with the following cannot be disclosed pursuant to § 164.512(f)(2): DNA data and analyses; dental records; or typing, samples or analyses of tissues or bodily fluids other than blood (*e.g.,* saliva). If a covered entity discloses additional information under this provision, the covered entity will be out of compliance and subject to sanction.

We clarify our intent not to allow covered entities to initiate disclosures of limited identifying information to law enforcement in the absence of a law enforcement request; a covered entity may disclose protected health information under this provision only in response to a request from law enforcement. We allow a ''law enforcement official's request'' to be

made orally or in writing, and we intend for it to include requests by a person acting on behalf of law enforcement, for example, requests by a media organization making a television or radio announcement seeking the public's assistance in identifying a suspect. Such a request also may include a ''Wanted'' poster and similar postings.

Disclosure About a Victim of Crime

The NPRM would have allowed covered entities to disclose protected health information about a victim of a crime, abuse or other harm to a law enforcement official, if the law enforcement official represented that: (i) The information was needed to determine whether a violation of law by a person other than the victim had occurred; and (ii) immediate law enforcement activity that depended on obtaining the information may have been necessary.

The final rule modifies the conditions under which covered entities can disclose protected health information about victims. In addition, as discussed above, the final rule includes a new § 164.512(c), which establishes conditions for disclosure of protected health information about victims of abuse, neglect or domestic violence. In addition, as discussed above, we have added § 164.512(f)(1)(i) to this paragraph to explicitly recognize that in some cases, covered entities' disclosure of protected health information is mandated by state or other law. The rule's requirements for disclosure in situations not covered under mandatory reporting laws are different from the rule's provisions regarding disclosure pursuant to a mandatory reporting law.

The final rule requires covered entities to obtain individual agreement as a condition of disclosing the protected health information about victims to law enforcement, unless the disclosure is permitted under § 164.512(b) or (c) or § 164.512(f)(1) above. The required agreement may be obtained orally, and does not need to meet the requirements of § 164.508 of this rule (regarding authorizations). The rule waives the requirement for individual agreement if the victim is unable to agree due to incapacity or other emergency circumstance and: (1) The law enforcement official represents that the protected health information is needed to determine whether a violation of law by a person other than the victim has occurred and the information is not intended to be used against the victim; (2) the law enforcement official represents that immediate law enforcement activity that depends on such disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and (3) the covered entity, in the exercise of professional judgment, determines that the disclosure is in the individual's best interests. We intend that assessing the individual's best interests includes taking into account any further risk of harm to the individual. This provision does not allow covered entities to initiate disclosures of protected health information to law enforcement; the disclosure must be in response to a request from law enforcement.

We do not intend to create a new legal duty on the part of covered entities with respect to the safety of their patients. Rather, we intend to ensure that covered entities can continue to exercise their professional judgment in these circumstances, on a case-by-case basis, as they do today.

In some cases, a victim may also be a fugitive or suspect. For example, an individual may receive a gunshot wound during a robbery and seek treatment in a hospital emergency room. In such cases, when law enforcement officials are requesting protected health information because the individual is a suspect (and thus the information may be used against the individual), covered entities may disclose the protected health information pursuant to § 164.512(f)(2) regarding suspects and not pursuant to § 164.512(f)(3) regarding victims. Thus, in these situations, covered entities may disclose only the limited identifying information listed in § 164.512(f)(2)—not all of the protected health information that may be disclosed under § 164.512(f)(3).

The proposed rule did not address whether a covered entity could disclose protected health information to a law enforcement official to alert the official of the individual's death.

Disclosures About Decedents

In the final rule, we add a new provision § 164.512(f)(4) in which we permit covered entities to disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death if the covered entity has a suspicion that such death may have resulted from criminal conduct. In such circumstances consent of the individual is not available and it may be difficult to determine the identity of a personal representative and gain consent for disclosure of protected health information. Permitting disclosures in this circumstance will permit law enforcement officials to begin their investigation into the death more rapidly, increasingly the likelihood of success.

Intelligence and National Security Activities

Section 164.510(f)(4) of the NPRM would have allowed covered entities to disclose protected health information to a law enforcement official without individual authorization for the conduct of lawful intelligence activities conducted pursuant to the National Security Act of 1947 (50 U.S.C. 401 *et seq.*) or in connection with providing protective services to the President or other individuals pursuant to section 3056 of title 18, United States Code. In the final rule, we move provisions regarding disclosures of protected health information for intelligence and protective services activities to § 164.512(k) regarding uses and disclosures for specialized government functions.

Criminal Conduct on the Premises of a Covered Entity

The NPRM would have allowed covered entities on their own initiative to disclose to law enforcement officials protected health information that the covered entity believed in good faith constituted evidence of criminal conduct that arose out of and was directly related to: (A) The receipt of health care or payment for health care, including a fraudulent claim for health care; (B) qualification for or receipt of benefits, payments, or services based on a fraudulent statement or material misrepresentation of the health of the individual; that occurred on the covered entity's premises or was witnessed by a member of the covered entity's workforce.

In the final rule, we modify this provision substantially, by eliminating language allowing disclosures already permitted in other sections of the regulation. The proposed provision overlapped with other sections of the NPRM, in particular proposed § 164.510(c) regarding disclosure for health oversight activities. In the final regulation, we clarify that this provision applies only to disclosures to law enforcement officials of protected health information that the covered entity believes in good faith constitutes evidence of a crime committed on the premises. We eliminate proposed § 164.510(f)(5)(i) regarding health care fraud from the law enforcement section, because all disclosures that would have been allowed under that provision are allowed under § 164.512(d) of the final rule (health oversight). Similarly, in the final rule, we eliminate proposed

§ 164.510(f)(5)(iii) on disclosure of protected health information to law enforcement officials regarding criminal activity witnessed by a member of a health plan workforce. All disclosures that would have been permitted by that provision are included in § 164.512(f)(5), which allows disclosure of information to report a crime committed on the covered entity's premises, and by § 164.502, which provides that a covered entity is not in violation of the rule when a member of its workforce or person working for a business associate uses or discloses protected health information while acting as a ''whistle blower.'' Thus, § 164.512(f)(5) allows covered entities to disclose health information only on the good faith belief that it constitutes evidence of a crime on their premises. The preamble to the NPRM said that if the covered entity disclosed protected health information in good faith but was wrong in its belief that the information was evidence of a violation of law, the covered entity would not be subject to sanction under this regulation. The final rule retains this approach.

Reporting Crime in Emergencies

The proposed rule did not address disclosures by emergency medical personnel to a law enforcement official intended to alert law enforcement about the commission of a crime. Because the provisions of proposed rule were limited to individually identifiable health information that was reduced to electronic form, many communications that occur between emergency medical personnel and law enforcement officials at the scene of a crime would not have been covered by the proposed provisions.

In the final rule we include a new provision § 164.512(f)(6) that addresses ''911'' calls for emergency medical technicians as well as other emergency health care in response to a medical emergency. The final rule permits a covered health care provider providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, to disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to (1) the commission and nature of a crime, (2) the location of such crime or of the victim(s) of such crime, and (3) the identity, description, and location of the perpetrator of such crime. A disclosure is not permitted under this section if health care provider believes that the medical emergency is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care. In such cases, disclosures to law enforcement would be governed by paragraph (c) of this section.

This added provision recognizes the special role of emergency medical technicians and other providers who respond to medical emergencies. In emergencies, emergency medical personnel often arrive on the scene before or at the same time as police officers, firefighters, and other emergency response personnel. In these cases, providers may be in the best position, and sometimes be the only ones in the position, to alert law enforcement about criminal activity. For instance, providers may be the first persons aware that an individual has been the victim of a battery or an attempted murder. They may also be in the position to report in real time, through use of radio or other mechanism, information that may immediately contribute to the apprehension of a perpetrator of a crime.

We note that disclosure under this provision is at the discretion of the health care provider. Disclosures in some instances may be governed more strictly, such as by applicable ethical standards and state and local laws.

Finally, the NPRM also included a proposed § 164.510(f)(5), which duplicated proposed § 164.510(f)(3). The final rule does not include this duplicate provision.

Additional Considerations

As stated in the NPRM, this paragraph is not intended to limit or preclude a covered entity from asserting any lawful defense or otherwise contesting the nature or scope of the process when the procedural rules governing the proceeding so allow. At the same time, it is not intended to create a basis for appealing to federal court concerning a request by state law enforcement officials. Each covered entity will continue to have available legal procedures applicable in the appropriate jurisdiction to contest such requests where warranted.

As was the case with the NPRM, this rule does not create any new affirmative requirement for disclosure of protected health information. Similarly, this section is not intended to limit a covered entity from disclosing protected health information to law enforcement officials where other sections of the rule permit such disclosure, *e.g.*, as permitted by § 164.512(j) to avert an imminent threat to health or safety, for health oversight activities, to coroners or medical examiners, and in other circumstances permitted by the rule. For additional provisions permitting covered entities to disclose protected health information to law enforcement officials, see § 164.512(j)(1)(i) and (ii).

Under the NPRM and under the final rule, to obtain protected health information, law enforcement officials must comply with whatever other law is applicable. In certain circumstances, while this provision could authorize a covered entity to disclose protected health information to law enforcement officials, there could be additional applicable statutes or rules that further govern the specific disclosure. If the preemption provisions of this regulation do not apply, the covered entity must comply with the requirements or limitations established by such other law, regulation or judicial precedent. See §§ 160.201 through 160.205. For example, if state law permits disclosure only after compulsory process with court review, a provider or payor is not allowed to disclose information to state law enforcement officials unless the officials have complied with that requirement. Similarly, disclosure of substance abuse patient records subject to, 42 U.S.C. 290dd–2, and the implementing regulations, 42 CFR part 2, continue to be governed by those provisions.

In some instances, disclosure of protected health information to law enforcement officials will be compelled by other law, for example, by compulsory judicial process or compulsory reporting laws (such as laws requiring reporting of wounds from violent crimes, suspected child abuse, or suspected theft of controlled substances). As discussed above, disclosure of protected health information under such other mandatory law is permitted under § 164.512(a).

In the responses to comments we clarify that items such as cells and tissues are not protected health information, but that analyses of them is. The same treatment would be given other physical items, such as clothing, weapons, or a bloody knife. We note, however, that while these items are not protected health information and may be disclosed, some communications that could accompany the disclosure will be protected health information under the rule. For example, if a person provides cells to a researcher, and tells the researcher that these are an identified individual's cancer cells, that accompanying statement is protected health information about that individual. Similarly, if a person provides a bullet to law enforcement, and tells law enforcement that the bullet was extracted from an identified

individual, the person has disclosed the fact that the individual was treated for a wound, and the additional statement is a disclosure of protected health information.

To be able to make the additional statement accompanying the provision of the bullet, a covered entity must look to the rule to find a provision under which a disclosure may be made to law enforcement. Section 164.512(f) of the rule addresses disclosures for law enforcement purposes. Under § 164.512(f)(1), the additional statement may be disclosed to a law enforcement official if required by law or with appropriate process. Under § 164.512(f)(2), we permit covered entities to disclose limited identifying information without legal process in response to a request from a law enforcement official for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person. Thus, in the case of bullet described above, the covered entity may, in response to a law enforcement request, provide the extracted bullet and such additional limited identifying information as is permitted under § 164.512(f)(2).

Section 164.512(g)—Uses and Disclosures About Decedents

In the NPRM we proposed to allow covered entities to disclose protected health information without individual authorization to coroners and medical examiners, consistent with applicable law, for identification of a deceased person or to determine cause of death.

In § 164.512(g) of the final rule, we permit covered entities to disclose protected health information to coroners, medical examiners, and funeral directors as part of a new paragraph on disclosures related to death. The final rule retains the NPRM approach regarding disclosure of protected health information to coroners and medical examiners, and it allows the information disclosed to coroners and medical examiners to include identifying information about other persons that may be included in the individual's medical record. Redaction of such names is not required prior to disclosing the individual's record to coroners or medical examiners. Since covered entities may also perform duties of a coroner or medical examiner, where a covered entity is itself a coroner or medical examiner, the final rule permits the covered entity to use protected health information in all cases in which it is permitted to disclose such information for its duties as a coroner or medical examiner.

Section 164.512(g) allows covered entities to disclose protected health information to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to a decedent. For example, the rule allows hospitals to disclose to funeral directors the fact that an individual has donated an organ or tissue, because this information has implications for funeral home staff duties associated with embalming. When necessary for funeral directors to carry out their duties, covered entities may disclose protected health information prior to and in reasonable anticipation of the individual's death.

Whereas the NPRM did not address the issue of disclosure of psychotherapy notes without individual authorization to coroners and medical examiners, the final rule allows such disclosures.

The NPRM did not include in proposed § 164.510(e) language stating that where a covered entity was itself a coroner or medical examiner, it could use protected health information for the purposes of engaging in a coroner's or a medical examiner's activities. The final rule includes such language to address situations such as where a public hospital performs medical examiner functions. In such cases, the hospital's on-staff coroners can use protected health information while conducting post-mortem investigations, and other hospital staff can analyze any information associated with these investigations, for example, as part of the process of determining the cause of the individual's death.

Section 164.512(h)—Uses and Disclosures for Cadaveric Donation of Organs, Eyes, or Tissues

In the NPRM we proposed to include the procurement or banking of blood, sperm, organs, or any other tissue for administration to patients in the definition of ''health care'' (described in proposed § 160.103). The NPRM's proposed approach did not differentiate between situations in which the donor was competent to consent to the donation—for example, when an individual is donating blood, sperm, a kidney, or a liver or lung lobe—and situations in which the donor was deceased, for example, when cadaveric organs and tissues were being donated. We also proposed to allow use and disclosure of protected health information for treatment without consent.

In the final rule, we take a different approach. In § 164.512(h), we permit covered entities to disclose protected health information without individual authorization to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for donation and transplantation. This provision is intended to address situations in which an individual has not previously indicated whether he or she seeks to donate organs, eyes, or tissues (and therefore authorized release of protected health information for this purpose). In such situations, this provision is intended to allow covered entities to initiate contact with organ and tissue donation and transplantation organizations to facilitate transplantation of cadaveric organs, eyes, and tissues.

Disclosures and Uses for Government Health Data Systems

In the NPRM we proposed to permit covered entities to disclose protected health information to a government agency, or to a private entity acting on behalf of a government agency, for inclusion in a government health data system collecting health data for analysis in support of policy, planning, regulatory, or management functions authorized by law. The NPRM stated that when a covered entity was itself a government agency collecting health data for these functions, it could use protected health information in all cases for which it was permitted to disclose such information to government health data systems.

In the final rule, we eliminate the provision that would have allowed covered entities to disclose protected health information to government health data systems without authorization. Thus, under the final rule, covered entities cannot disclose protected health information without authorization to government health data systems—or to private health data systems—unless the disclosure is permissible under another provision of the rule.

Disclosures for Payment Processes

In the NPRM we proposed to permit covered entities to disclose, in connection with routine banking activities or payment by debit, credit, or other payment card, or other payment means, the minimum amount of protected health information necessary to complete a banking or payment activity to financial institutions or to entities acting on behalf of financial institutions to authorize, process, clear, settle, bill, transfer, reconcile, or collect payments for financial institutions.

The preamble to the NPRM clarified the proposed rule's intent regarding disclosure of diagnostic and treatment information along with payment

information to financial institutions. The preamble to the proposed rule said that diagnostic and treatment information never was necessary to process a payment transaction. The preamble said we believed that in most cases, the permitted disclosure would include only: (1) The name and address of the account holder; (2) the name and address of the payor or provider; (3) the amount of the charge for health services; (4) the date on which health services were rendered; (5) the expiration date for the payment mechanism, if applicable; and (6) the individual's signature. The preamble noted that the proposed regulation text did not include an exclusive list of information that could lawfully be disclosed to process payments, and it solicited comments on whether more elements would be needed for banking and payment transactions and on whether including a specific list of protected health information that could be disclosed was an appropriate approach.

The preamble also noted that under section 1179 of HIPAA, certain activities of financial institutions were exempt from this rule, to the extent that these activities constituted authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments for health care or health plan premiums.

In the final rule, we eliminate the NPRM's provision on ''banking and payment processes.'' All disclosures that would have been allowed pursuant to proposed § 164.510(i) are allowed under § 164.502(a) of the final rule, regarding disclosure for payment purposes.

Section 164.512(i)—Uses and Disclosures for Research Purposes

The NPRM would have permitted covered entities to use and disclose protected health information for research—regardless of funding source—without individual authorization, provided that the covered entity obtained documentation of the following:

(1) A waiver, in whole or in part, of authorization for the use or disclosure of protected health information was approved by an Institutional Review Board (IRB) or a privacy board that was composed as stipulated in the proposed rule;

(2) The date of approval of the waiver, in whole or in part, of authorization by an IRB or privacy board;

(3) The IRB or privacy board had determined that the waiver, in whole or in part satisfied the following criteria:

(i) The use or disclosure of protected health information involves no more than minimal risk to the subjects;

(ii) The waiver will not adversely affect the rights and welfare of the subjects;

(iii) The research could not practicably be conducted without the waiver;

(iv) Whenever appropriate, the subjects will be provided with additional pertinent information after participation;

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

(vi) The research is of sufficient importance so as to outweigh the intrusion of the privacy of the individual whose information is subject to the disclosure;

(vii) There is an adequate plan to protect the identifiers from improper use and disclosure; and

(viii) There is an adequate plan to destroy the identifiers at the earliest opportunity consistent with the conduct of the research, unless there is a health or research justification for retaining the identifiers; and

(4) The written documentation was signed by the chair of, as applicable, the IRB or the privacy board.

The NPRM also proposed that IRBs and privacy boards be permitted to adopt procedures for ''expedited review'' similar to those provided in the Common Rule (Common Rule § .110) for records research that involved no more than minimal risk. However, this provision for expedited review was not included in the proposed regulation text.

The board that would determine whether the research protocol met the eight specified criteria for waiving the patient authorization requirements (described above), could have been an IRB constituted as required by the Common Rule, or a privacy board, whose proposed composition is described below. The NPRM proposed no requirements for the location or sponsorship of the IRB or privacy board. Under the NPRM, the covered entity could have created such a board and could have relied on it to review research proposals for uses and disclosures of protected health information for research. A covered entity also could have relied on the necessary documentation from an outside researcher's own university IRB or privacy board. In addition, a covered entity could have engaged the services of an outside IRB or privacy board to obtain the necessary documentation.

Absent documentation that the requirements described above had been met, the NPRM would have required individuals' authorization for the use or disclosure of protected health information for research, pursuant to the authorization requirements in proposed § 164.508. For research conducted with patient authorization, documentation of IRB or privacy board approval would not have been required.

The final rule retains the NPRM's proposed framework for permitting uses and disclosures of protected health information for research purposes, although we are making several important changes for the final rule. These changes are discussed below:

Documentation Requirements of IRB or Privacy Board Approval of Waiver

The final rule retains these documentation requirements, but modifies some of them and includes two additional documentation requirements. The final rule's modifications to the NPRM's proposed documentation requirements are described first, followed by a description of the three documentation requirements added in the final rule.

The final rule makes the following modifications to the NPRM's proposed documentation requirements for the waiver of individual authorization:

1. *IRB and privacy board membership.* The NPRM stipulated that to meet the requirements of proposed § 164.510(j), the documentation would need to indicate that the IRB had been composed as required by the Common Rule (§ .107), and the privacy board had been composed as follows: ''(A) Has members with varying backgrounds and appropriate professional competency as necessary to review the research protocol; (B) Includes at least one member who is not affiliated with the entity conducting the research, or related to a person who is affiliated with such entity; and (C) Does not have any member participating in a review of any project in which the member has a conflict of interest'' (§ 164.510(j)(1)(ii)).

The final rule modifies the first of the requirements for the composition of a privacy board to focus on the effect of the research protocol on the individual's privacy rights and related interests. Therefore, under the final rule, the required documentation must indicate that the privacy board has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests.

In addition, the final rule further restricts the NPRM's proposed requirement that the privacy board include at least one member who was

not affiliated with the entity conducting the research, or related to a person who is affiliated with such entity. Under the final rule, the board must include at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with such entities.

The other documentation requirements for the composition of an IRB and privacy board remain the same.

2. *Waiver of authorization criteria.* The NPRM proposed to prohibit the use or disclosure of protected health information for research without individual authorization as stipulated in proposed § 164.508 unless the covered entity had documentation indicating that an IRB or privacy board had determined that the following waiver criteria had been met:

(i) The use or disclosure of protected health information involves no more than minimal risk to the subjects;

(ii) The waiver will not adversely affect the rights and welfare of the subjects;

(iii) The research could not practicably be conducted without the waiver;

(iv) Whenever appropriate, the subjects will be provided with additional pertinent information after participation;

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

(vi) The research is of sufficient importance so as to outweigh the intrusion of the privacy of the individual whose information is subject to the disclosure;

(vii) There is an adequate plan to protect the identifiers from improper use and disclosure; and

(viii) There is an adequate plan to destroy the identifiers at the earliest opportunity consistent with the conduct of the research, unless there is a health or research justification for retaining the identifiers.

The final rule continues to permit the documentation of IRB or privacy board approval of a waiver of an authorization as required by § 164.508, to indicate that only some or all of the § 164.508 authorization requirements have been waived. In addition, the final rule clarifies that the documentation of IRB or privacy board approval may indicate that the authorization requirements have been altered. Also, for all of the proposed waiver of authorization criteria that used the term ''subject,'' we replace this term with the term ''individual'' in the final rule.

In addition, the final rule (1) eliminates proposed waiver criterion iv, (2) modifies proposed waiver criteria ii, iii, vi, and viii, and (3) adds a waiver criterion.

Proposed waiver criterion ii (waiver criterion § 164.512(i)(2)(ii)(B) in the final rule) is revised as follows to focus more narrowly on the privacy interests of individuals, and to clarify that it also pertains to alterations of individual authorization: ''the alteration or waiver will not adversely affect the privacy rights and the welfare of the individuals.'' Under criterion § 164.512(i)(2)(ii)(B), the question is whether the alteration or waiver of individual authorization would adversely affect the privacy rights and the welfare of individuals, not whether the research project itself would adversely affect the privacy rights or the welfare of individuals.

Proposed waiver criterion iii (waiver criterion § 164.512(i)(2)(ii)(C) in the final rule) is revised as follows to clarify that it also pertains to alterations of individual authorization: ''the research could not practicably be conducted without the alteration or waiver.''

Proposed waiver criterion vi (waiver criterion § 164.512(i)(2)(ii)(E) in the final rule) is revised as follows to be more consistent with one of the Common Rule's requirements for the approval of human subjects research (Common Rule, § .111(a)(2)): ''the privacy risks to individuals whose protected health information is to be used or disclosed are reasonable in relation to anticipated benefits if any to individuals, and the importance of the knowledge that may reasonably be expected to result from the research.'' Under criterion § 164.512(i)(2)(ii)(E), the question is whether the risks to an individual's privacy from participating in the research are reasonable in relation to the anticipated benefits from the research. This criterion is unlike waiver criterion § 164.512(i)(2)(ii)(B) in that it focuses on the privacy risks and benefits of the research project more broadly, not on the waiver of individual authorization.

Proposed waiver criterion viii (waiver criterion § 164.512(i)(2)(ii)(G) in the final rule) is revised as follows: ''there is an adequate plan to destroy the identifiers at the earliest opportunity consistent with the conduct of the research, unless there is a health or research justification for retaining the identifiers, or such retention is otherwise required by law.''

In addition, the final rule includes another waiver criterion: waiver criterion § 164.512(i)(2)(ii)(H). The NPRM proposed no restriction on a researcher's further use or disclosure of protected health information that had been received under proposed § 164.510(j). The final rule requires that the covered entity obtain written agreement from the person or entity receiving protected health information under § 164.512(i) not to re-use or disclose protected health information to any other person or entity, except: (1) As required by law, (2) for authorized oversight of the research project, or (3) for other research for which the use or disclosure of protected health information would be permitted by this subpart. For instance, in assessing whether this criterion has been met, we encourage IRBs and privacy boards to obtain adequate assurances that the protected health information will not be disclosed to an individual's employer for employment decisions without the individual's authorization.

3. *Required signature.* The rule broadens the types of individuals who are permitted to sign the required documentation of IRB or privacy board approval. The final rule requires the documentation of the alteration or waiver of authorization to be signed by (1) the chair of, as applicable, the IRB or the privacy board, or (2) a member of the IRB or privacy board, as applicable, who is designated by the chair to sign the documentation.

Furthermore, the final rule makes the following three additions to the proposed documentation requirements for the alteration or waiver of authorization:

1. *Identification of the IRB or privacy board.* The NPRM did not propose that the documentation of waiver include a statement identifying the IRB or privacy board that approved the waiver of authorization. In the final rule we require that such a statement be included in the documentation of alteration or waiver of individual authorization. By this requirement we mean that the name of the IRB or privacy board must be included in such documentation, not the names of individual members of the board.

2. *Description of protected health information approved for use or disclosure.* The NPRM did not propose that the documentation of waiver include a description of the protected health information that the IRB or privacy board had approved for use or disclosure without individual authorization. In considering waiver of authorization criterion § 164.512(i)(2)(ii)(D), we expect the IRB or privacy board to consider the amount of information that is minimally needed for the study. The final rule requires that the documentation of IRB or

privacy board approval of the alteration or waiver of authorization describe the protected health information for which use or access has been determined to be necessary for the research by the IRB or privacy board. For example, if the IRB or privacy board approves only the use or disclosure of certain information from patients' medical records, and not patients' entire medical record, this must be stated on the document certifying IRB or privacy board approval.

3. *Review and approval procedures.* The NPRM would not have required documentation of IRBs' or privacy boards' review and approval procedures. In the final rule, the documentation of the alteration or waiver of authorization must state that the alteration or waiver has been reviewed and approved by: (1) an IRB that has followed the voting requirements stipulated in the Common Rule (§ .108(b)), or the expedited review procedures as stipulated in § .110(b); or (2) a privacy board that has reviewed the proposed research at convened meetings at which a majority of the privacy board members are present, including at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any such entities, and the alteration or waiver of authorization is approved by the majority of privacy board members present at the meeting, unless an expedited review procedure is used.

For documentation of IRB approval that used an expedited review procedure, the covered entity must ensure that the documentation indicates that the IRB followed the expedited review requirements of the Common Rule (§ .110). For documentation of privacy board approval that used an expedited review procedure, the covered entity must ensure that the documentation indicates that the privacy board met the expedited review requirements of the privacy rule. In the final rule, a privacy board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the protected health information for which disclosure is being sought. If a privacy board elects to use an expedited review procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the privacy board, or by one or more members of the privacy board as designated by the chair. Use of the expedited review mechanism permits review by a single member of the IRB or privacy board, but continues to require that the covered entity obtain documentation that all of the specified waiver criteria have been met.

Reviews Preparatory to Research

Under the NPRM, if a covered entity used or disclosed protected health information for research, but the researcher did not record the protected health information in a manner that persons could be identified, such an activity would have constituted a research use or disclosure that would have been subject to either the individual authorization requirements of proposed § 164.508 or the documentation of the waiver of authorization requirements of proposed § 164.510(j).

The final rule permits the use and disclosure of protected health information for research without requiring authorization or documentation of the alteration or waiver of authorization, if the research is conducted in such a manner that only de-identified protected health information is recorded by the researchers and the protected health information is not removed from the premises of the covered entity. For such uses and disclosures of protected health information, the final rule requires that the covered entity obtain from the researcher representations that use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research, no protected health information is to be removed from the covered entity by the researcher in the course of the review, and the protected health information for which use or access is sought is necessary for the research purposes. The intent of this provision is to permit covered entities to use and disclose protected health information to assist in the development of a research hypothesis and aid in the recruitment of research participants. We understand that researchers sometimes require access to protected health information to develop a research protocol, and to determine whether a specific covered entity has protected health information of prospective research participants that would meet the eligibility criteria for enrollment into a research study. Therefore, this provision permits covered entities to use and disclose protected health information for these preliminary research activities without individual authorization and without documentation that an IRB or privacy board has altered or waived individual authorization.

Research on Protected Health Information of the Deceased

The NPRM would have permitted the use and disclosure of protected health information of deceased persons for research without the authorization of a legal representative, and without the requirement for written documentation of IRB or privacy board approval in proposed § 164.510(j). In the final rule, we retain the exception for uses and disclosures for research purposes but in addition require that the covered entity take certain protective measures prior to release of the decedent's protected health information for such purposes. Specifically, the final rule requires that the covered entity obtain representation that the use or disclosure is sought solely for research on the protected health information of decedent, and representation that the protected health information for which use or disclosure is sought is necessary for the research purposes. In addition, the final rule allows covered entities to request from the researcher documentation of the death of the individuals about whom protected health information is being sought.

Good Faith Reliance

The final rule clarifies that covered entities are allowed to rely on the IRB's or privacy board's representation that the research proposal meets the documentation requirements of § 164.512(i)(1)(i) and the minimum necessary requirements of § 164.514.

In addition, when using or disclosing protected health information for reviews preparatory to research (§ 164.512(i)(1)(ii)) or for research solely on the protected health information of decedents (§ 164.512)(1)(iii)), the final rule clarifies that the covered entity may rely on the requesting researcher's representation that the purpose of the request is for one of these two purpose, and that the request meets the minimum necessary requirements of § 164.514. Therefore, the covered entity has not violated the rule if the requesting researcher misrepresents his or her intended use of the protected health information to the covered entity.

Additional Research Provisions

Research Including Treatment

To the extent that a researcher provided treatment to persons as part of a research study, the NPRM would have covered such researchers as health care providers for purposes of that treatment, and required that the researcher comply with all of the provisions of the rule that

would be applicable to health care providers. The final rule retains this requirement.

Individual Access to Research Information

Under proposed § 164.514, the NPRM would have applied the proposed provision regarding individuals' access to records to research that includes the delivery of treatment. The NPRM proposed an exception to individuals' right to access protected health information for clinical trials, where (1) protected health information was obtained by a covered entity in the course of clinical trial, (2) the individual agreed to the denial of access when consenting to participate in the trial (if the individual's consent to participate was obtained), and (3) the trial was still in progress.

Section 164.524 of the final rule retains this exception to access for research that includes treatment. In addition, the final rule requires that participants in such research be informed that their right of access to protected health information about them will be reinstated once the research is complete.

Obtaining the Individual's Authorization for Research

The NPRM would have required covered entities obtaining individuals' authorization for the use or disclosure of information for research to comply with the requirements applicable to individual authorization for the release of protected health information (proposed § 164.508(a)(2)). If an individual had initiated the use or disclosure of his/her protected health information for research, or any other purpose, the covered entity would have been required to obtain a completed authorization for the use or disclosure of protected health information as proposed in § 164.508(c).

The final rule retains these requirements for research conducted with authorization, as required by § 164.508. In addition, for the use and disclosure of protected health information created by a covered entity for the purpose, in whole or in part, of research that includes treatment of the individual, the covered entity must meet the requirements of § 164.508(f).

Interaction with the Common Rule

The NPRM stated that the proposed rule would not override the Common Rule. Where both the NPRM and the Common Rule would have applied to research conducted by the covered entity—either with or without individuals' authorization—both sets of regulations would have needed to be followed. This statement remains true in the final rule. In addition, we clarify that FDA's human subjects regulations must also be followed if applicable.

Section 164.512(j)—Uses and Disclosures to Avert a Serious Threat to Health or Safety

In the NPRM we proposed to allow covered entities to use or disclose protected health information without individual authorization—consistent with applicable law and ethics standards—based on a reasonable belief that use or disclosure of the protected health information was necessary to prevent or lessen a serious and imminent threat to health or safety of an individual or of the public. Pursuant to the NPRM, covered entities could have used or disclosed protected health information in these emergency circumstances to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat. The NPRM stated that covered entities that made disclosures in these circumstances were presumed to have acted under a reasonable belief if the disclosure was made in good faith, based on credible representation by a person with apparent knowledge or authority. The NPRM did not include verification requirements specific to this paragraph.

In § 164.512(j) of the final rule, we retain the NPRM's approach to uses and disclosures made to prevent or lessen serious and imminent threats to health or safety, as well as its language regarding the presumption of good faith. We also clarify that: (1) Rules governing these situations, which the NPRM referred to as ''emergency circumstances,'' are not intended to apply to emergency care treatment, such as health care delivery in a hospital emergency room; and (2) the ''presumption of good faith belief'' is intended to apply only to this provision and not to all disclosures permitted without individual authorization. The final rule allows covered entities to use or disclose protected health information without an authorization on their own initiative in these circumstances, when necessary to prevent or lessen a serious and imminent threat, consistent with other applicable ethical or legal standards.

The rule's approach is consistent with the ''duty to warn'' third persons at risk, which has been established through case law. In *Tarasoff* v. *Regents of the University of California* (17 Cal. 3d 425 (1976)), the Supreme Court of California found that when a therapist's patient had made credible threats against the physical safety of a specific person, the therapist had an obligation to use reasonable care to protect the intended victim of his patient against danger, including warning the victim of the danger. Many states have adopted, through either statutory or case law, versions of the Tarasoff duty to warn. The rule is not intended to create a duty to warn or disclose. Rather, it permits disclosure to avert a serious and imminent threat to health or safety consistent with other applicable legal or ethical standards. If disclosure in these circumstances is prohibited by state law, this rule would not allow the disclosure.

As indicated above, in some situations (for example, when a person is both a fugitive and a victim and thus covered entities could disclose protected health information pursuant either to § 164.512(f)(2) regarding fugitives or to § 164.512(f)(3) establishing conditions for disclosure about victims), more than one section of this rule potentially could apply with respect to a covered entity's potential disclosure of protected health information. Similarly, in situations involving a serious and imminent threat to public health or safety, law enforcement officials may be seeking protected health information from covered entities to locate a fugitive. In the final rule, we clarify that if a situation fits one section of the rule (for example, § 164.512(j) on serious and imminent threats to health or safety), covered entities may disclose protected health information pursuant to that section, regardless of whether the disclosure also could be made pursuant to another section (*e.g.,* § 164.512(f)), regarding disclosure to law enforcement officials).

The proposed rule did not address situations in which covered entities could make disclosures to law enforcement officials about oral statements admitting participation in violent conduct or about escapees.

In the final rule we permit, but do not require, covered entities to use or disclose protected health information, consistent with applicable law and standards of ethical conduct, in specific situations in which the covered entity, in good faith, believes the use or disclosure is necessary to permit law enforcement authorities to identify or apprehend an individual. Under paragraph (j)(1)(ii)(A) of this section, a covered entity may take such action because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have resulted in serious physical harm to the victim. The

protected health information that is disclosed in this case is limited to the statement and to the protected health information included under the limited identifying and location information in § 164.512(f)(2), such as name, address, and type of injury. Under paragraph (j)(1)(ii)(B) of this section, a covered entity may take such action where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody.

A disclosure may not be made under paragraph (j)(1)(ii)(A) for a statement admitting participation in a violent crime if the covered entity learns the information in the course of counseling or therapy. Similarly, such a disclosure is not permitted if the covered entity learns the information in the course of treatment to affect the propensity to commit the violent crimes that are described in the individual's statements. We do not intend to discourage individuals from speaking accurately in the course of counseling or therapy sessions, or to discourage other treatment that specifically seeks to reduce the likelihood that someone who has acted violently in the past will do so again in the future. This prohibition on disclosure is triggered once an individual has made a request to initiate or be referred to such treatment, therapy, or counseling.

The provision permitting use and disclosure has been added in light of the broadened definition in the final rule of protected health information. Under the NPRM, protected health information meant individually identifiable health information that is or has been electronically transmitted or electronically maintained by a covered entity. Under the final rule, protected health information includes information transmitted by electronic media as well as such information transmitted or maintained in any other form or medium. The new definition includes oral statements to covered entities as well as individually identifiable health information transmitted ''in any other form.''

The definition of protected health information, for instance, would now apply to a statement by a patient that is overheard by a hospital security guard in a waiting room. Such a statement would have been outside the scope of the proposed rule (unless it was memorialized in an electronic record), but is within the scope of the final rule. For the example with the hospital guard, the new provision permitting disclosure of a statement by an individual admitting participation in a violent crime would have the same effect as the proposed rule—the statement could be disclosed to law enforcement, so long as the other aspects of the regulation are followed. Similarly, where it appears from all the circumstances that the individual has escaped from prison, the expanded definition of protected health information should not prevent the covered entity from deciding to report this information to law enforcement.

The disclosures that covered entities may elect to make under this paragraph are entirely at their discretion. These disclosures to law enforcement are in addition to other disclosure provisions in the rule. For example, under paragraph § 164.512(f)(2) of this section, a covered entity may disclose limited categories of protected health information in response to a request from a law enforcement official for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person. Paragraph § 164.512(f)(1) of this section permits a covered entity to make disclosures that are required by other laws, such as state mandatory reporting laws, or are required by legal process such as court orders or grand jury subpoena.

Section 164.512(k)—Uses and Disclosures for Specialized Government Functions

Application to Military Services

In the NPRM we would have permitted a covered entity providing health care to Armed Forces personnel to use and disclose protected health information for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, where the appropriate military authority had published by notice in the **Federal Register** (In the NPRM, we proposed that the Department of Defense would publish this **Federal Register** notice in the future.) The final rule takes a similar approach while making some modifications to the NPRM. One modification concerns the information that will be required in the **Federal Register** notice. The NPRM would have required a listing of (i) appropriate military command authorities; (ii) the circumstances for which use or disclosure without individual authorization would be required; and (iii) activities for which such use or disclosure would occur in order to assure proper execution of the military mission. In the final rule, we eliminate the third category and also slightly modify language in the second category to read: ''the purposes for which the protected health information may be used or disclosed.''

An additional modification concerns the rule's application to foreign military and diplomatic personnel. The NPRM would have excluded foreign diplomatic and military personnel, as well as their dependents, from the proposed definition of ''individual,'' thereby excluding any protected health information created about these personnel from the NPRM's privacy protections. Foreign military and diplomatic personnel affected by this provision include, for example, allied military personnel who are in the United States for training. The final rule applies a more limited exemption to foreign military personnel only (Foreign diplomatic personnel will have the same protections granted to all other individuals under the rule). Under the final rule, foreign military personnel are not excluded from the definition of ''individual.'' Covered entities will be able to use and disclose protected health information of foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for U.S. Armed Forces personnel under the notice to be published in the **Federal Register**. Foreign military personnel do have the same rights of access, notice, right to request privacy protection, copying, amendment, and accounting as do other individuals pursuant to §§ 164.520–164.526 (sections on access, notice, right to request privacy protection for protected health information, amendment, inspection, copying) of the rule.

The NPRM likewise would have exempted overseas foreign national beneficiaries from the proposed rule's requirements by excluding them from the definition of ''individual.'' Under the final rule, these beneficiaries no longer are exempt from the definition of ''individual.'' However, the rule's provisions do not apply to the individually identifiable health information of overseas foreign nationals who receive care provided by the Department of Defense, other federal agencies, or by non-governmental organizations incident to U.S. sponsored missions or operations.

The final rule includes a new provision to address separation or discharge from military service. The preamble to the NPRM noted that upon completion of individuals' military service, DOD and the Department of Transportation routinely transfer entire military service records, including protected health information to the Department of Veterans Affairs so that

the file can be retrieved quickly if the individuals or their dependents apply for veterans benefits. The NPRM would have required consent for such transfers. The final rule no longer requires consent in such situations. Thus, under the final rule, a covered entity that is a component of DOD or the Department of Transportation may disclose to DVA the protected health information of an Armed Forces member upon separation or discharge from military service for the purpose of a determination by DVA of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs.

Department of Veterans Affairs

Under the NPRM, a covered entity that is a component of the Department of Veterans Affairs could have used and disclosed protected health information to other components of the Department that determine eligibility for, or entitlement to, or that provide benefits under the laws administered by the Secretary of Veterans Affairs. In the final rule, we retain this approach.

Application to Intelligence Community

The NPRM would have provided an exemption from its proposed requirements to the intelligence community. As defined in section 4 of the National Security Act, 50 U.S.C. 401a, the intelligence community includes: the Office of the Director of Central Intelligence Agency; the Office of the Deputy Director of Central Intelligence; the National Intelligence Council and other such offices as the Director may designate; the Central Intelligence Agency; the National Security Agency; the Defense Intelligence Agency; the National Imagery and Mapping Agency ; the National Reconnaissance Office; other offices within the DOD for the collection of specialized national intelligence through reconnaissance programs; the intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Federal Bureau of Investigation, the Department of the Treasury, and the Department of Energy; the Bureau of Intelligence and Research of the Department of State; and such other elements of any other department or agency as may be designated by the President, or designated jointly by the Director of Central Intelligence and the head of the department or agency concerned, as an element of the intelligence community. It would have allowed a covered entity to use without individual authorization protected health information of employees of the intelligence community, and of their dependents, if such dependents were being considered for posting abroad. The final rule does not include such an exemption. Rather, the final rule does not except intelligence community employees and their dependents from the general rule requiring an authorization in order for protected health information to be used and disclosed.

National Security and Intelligence Activities

The NPRM included a provision, in § 164.510(f)—Disclosure for Law Enforcement Purposes—that would allow covered entities to disclose protected health information without consent for the conduct of lawful intelligence activities under the National Security Act, and in connection with providing protective services to the President or to foreign heads of state pursuant to 18 U.S.C. 3056 and 22 U.S.C. 2709(a)(3) respectively. The final rule preserves these exemptions, with slight modifications, but moves them from proposed § 164.510(f) to § 164.512(k). It also divides this area into two paragraphs—one called ''National Security and Intelligence Activities'' and the second called ''Protective services for the President and Others.''

The final rule, with modifications, allows a covered entity to disclose protected health information to an authorized federal official for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act and implementing authority (*e.g.,* Executive Order 1233). The references to ''counter-intelligence and other national security activities'' are new to the final rule. The reference to ''implementing authority (*e.g.* Executive Order 12333)'' is also new. The final rule also adds specificity to the provision on protective services. It states that a covered entity may disclose protected health information to authorized federal officials for the provision of protective services to the President or other persons as authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons as authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879.

Application to the State Department

The final rule creates a narrower exemption for Department of State for uses and disclosures of protected health information (1) for purposes of a required security clearance conducted pursuant to Executive Orders 10450 and 12698; (2) as necessary to meet the requirements of determining worldwide availability or availability for mandatory service abroad under Sections 101(a)(4) and 504 of the Foreign Service Act; and (3) for a family member to accompany a Foreign Service Officer abroad, consistent with Section 101(b)(5) and 904 of the Foreign Service Act.

Regarding security clearances, nothing prevents any employer from requiring that individuals provide authorization for the purpose of obtaining a security clearance. For the Department of State, however, the final rule provides a limited exemption that allows a component of the Department of State without an authorization to (1) use protected health information to make medical suitability determinations and (2) to disclose whether or not the individual was determined to be medically suitable to authorized officials in the Department of State for the purpose of a security clearance investigation conducted pursuant to Executive Order 10450 and 12698.

Sections 101(a)(4) and 504 of the Foreign Service Act require that Foreign Service members be available to serve in assignments throughout the world. The final rule permits disclosures to officials who need protected health information to determine availability for duty worldwide.

Section 101(b)(5) of the Foreign Service Act requires the Department of State to mitigate the impact of hardships, disruptions, and other unusual conditions on families of Foreign Service Officers. Section 904 requires the Department to establish a health care program to promote and maintain the physical and mental health of Foreign Service member family members. The final rule permits disclosure of protected health information to officials who need protected health information for a family member to accompany a Foreign Service member abroad.

This exemption does not permit the disclosure of specific medical conditions, diagnoses, or other specific medical information. It permits only the disclosure of the limited information needed to determine whether the individual should be granted a security clearance or whether the Foreign Service member of his or her family members should be posted to a certain overseas assignment.

Application to Correctional Facilities

The NPRM would have excluded the individually identifiable health information of correctional facility inmates and detention facility detainees from the definition of protected health information. Thus, none of the NPRM's

proposed privacy protections would have applied to correctional facility inmates or to detention facility detainees while they were in these facilities or after they had been released.

The final rule takes a different approach. First, to clarify that we are referring to individuals who are incarcerated in correctional facilities that are part of the criminal justice system or in the lawful custody of a law enforcement official—and not to individuals who are ''detained'' for non-criminal reasons, for example, in psychiatric institutions—§ 164.512(k) covers disclosure of protected health information to correctional institutions or law enforcement officials having such lawful custody. In addition, where a covered health care provider is also a health care component of a correctional institution, the final rule permits the covered entity to use protected health information in all cases in which it is permitted to disclose such information.

We define correctional institution as defined pursuant to 42 U.S.C. 13725(b)(1), as a ''prison, jail, reformatory, work farm, detention center, or halfway house, or any other similar institution designed for the confinement or rehabilitation of criminal offenders.'' The rules regarding disclosure and use of protected health information specified in § 164.512(k) cover individuals who are in transitional homes, and other facilities in which they are required by law to remain for correctional reasons and from which they are not allowed to leave. This section also covers individuals who are confined to psychiatric institutions for correctional reasons and who are not allowed to leave; however, it does not apply to disclosure of information about individuals in psychiatric institutions for treatment purposes only, who are not there due to a crime or under a mandate from the criminal justice system. The disclosure rules described in this section do not cover release of protected health information about individuals in pretrial release, probation, or on parole, such persons are not considered to be incarcerated in a correctional facility.

As described in § 164.512(k), correctional facility inmates' individually identifiable health information is not excluded from the definition of protected health information. When individuals are released from correctional facilities, they will have the same privacy rights that apply to all other individuals under this rule.

Section 164.512(k) of the final rule states that while individuals are in a correctional facility or in the lawful custody of a law enforcement official, covered entities (for example, the prison's clinic) can use or disclose protected health information about these individuals without authorization to the correctional facility or the law enforcement official having custody as necessary for: (1) The provision of health care to such individuals; (2) the health and safety of such individual or other inmates; (3) the health and safety of the officers of employees of or others at the correctional institution; and (4) the health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution or facility to another; (5) law enforcement on the premises of the correctional institution; and (6) the administration and maintenance of the safety, security, and good order of the correctional institution. This section is intended to allow, for example, a prison's doctor to disclose to a van driver transporting a criminal that the individual is a diabetic and frequently has seizures, as well as information about the appropriate action to take if the individual has a seizure while he or she is being transported.

We permit covered entities to disclose protected health information about these individuals if the correctional institution or law enforcement official represents that the protected health information is necessary for these purposes. Under 164.514(h), a covered entity may reasonably rely on the representation of such public officials.

Application to Public Benefits Programs Required to Share Eligibility Information

We create a new provision for covered entities that are a government program providing public benefits. This provision allows the following disclosures of protected health information.

First, where other law requires or expressly authorizes information relating to the eligibility for, or enrollment in more than one public program to be shared among such public programs and/or maintained in a single or combined data system, a public agency that is administering a health plan may maintain such a data base and may disclose information relating to such eligibility or enrollment in the health plan to the extent authorized by such other law.

Where another public entity has determined that the appropriate balance between the need for efficient administration of public programs and public funds and individuals' privacy interests is to allow information sharing for these limited purposes, we do not upset that determination. For example, section 1137 of the Social Security Act requires a variety of public programs, including the Social Security program, state medicaid programs, the food stamp program, certain unemployment compensation programs, and others, to participate in a joint income and eligibility verification system. Similarly, section 222 of the Social Security Act requires the Social Security Administration to provide information to certain state vocational rehabilitation programs for eligibility purposes. In some instances, it is a covered entity that first collects or creates the information that is then disclosed for these systems. We do not prohibit those disclosures.

This does not authorize these entities to share information for claims determinations or ongoing administration of these public programs. This provision is limited to the agencies and activities described above.

Second, § 164.512(k)(6) permits a covered entity that is a government agency administering a government program providing public benefits to disclose protected health information relating to the program to another covered entity that is a government agency administering a government program providing public benefits if the programs serve the same or similar populations and the disclosure of protected health information is necessary to coordinate the covered functions of such programs.

The second provision permits covered entities that are government program providing public benefits that serve the same or similar populations to share protected health information for the purposes of coordinating covered functions of the programs and for general management and administration relating to the covered functions of the programs. Often, similar government health programs are administered by different government agencies. For example, in some states, the Medicaid program and the State Children's Health Insurance Program are administered by different agencies, although they serve similar populations. Many states coordinate eligibility for these two programs, and sometimes offer services through the same delivery systems and contracts. This provision would permit the covered entities administering these programs to share protected health information of program participants to coordinate enrollment and services and to generally improve the health care operations of the programs. We note that this provision does not authorize the

agencies to use or disclose the protected health information that is shared for purposes other than as provided for in this paragraph.

Section 164.512(l)—Disclosures For Workers' Compensation

The NPRM did not contain special provisions permitting covered entities to disclose protected health information for the purpose of complying with workers' compensation and similar laws. Under HIPAA, workers' compensation and certain other forms of insurance (such as automobile or disability insurance) are ''excepted benefits.'' Insurance carriers that provide this coverage are not covered entities even though they provide coverage for health care services. To carry out their insurance functions, these non-covered insurers typically seek individually identifiable health information from covered health care providers and group health plans. In drafting the proposed rule, the Secretary was faced with the challenge of trying to carry out the statutory mandate of safeguarding the privacy of individually identifiable health information by regulating the flow of such information from covered entities while at the same time respecting the Congressional intent to shield workers' compensation carriers and other excepted benefit plans from regulation as covered entities.

In the proposed rule we allowed covered entities to disclose protected health information without individual consent for purposes of treatment, payment or health care operations—even when the disclosure was to a non-covered entity such as a workers' compensation carrier. In addition, we allowed protected health information to be disclosed if required by state law for purposes of determining eligibility for coverage or fitness for duty. The proposed rule also required that whenever a covered entity disclosed protected health information to a non-covered entity, even though authorized under the rule, the individual who was the subject of the information must be informed that the protected health information was no longer subject to privacy protections.

Like other disclosures under the proposed rule, the information provided to workers' compensation carriers for treatment, payment or health care operations was subject to the minimum necessary standard. However, to the extent that protected health information was disclosed to the carrier because it was required by law, it was not subject to the minimum necessary standard. In addition, individuals were entitled to an accounting when protected health information was disclosed for purposes other than treatment, payment or health care operations.

In the final rule, we include a new provision in this section that clarifies the ability of covered entities to disclose protected health information without authorization to comply with workers' compensation and similar programs established by law that provide benefits for work-related illnesses or injuries without regard to fault. Although most disclosures for workers' compensation would be permissible under other provisions of this rule, particularly the provisions that permit disclosures for payment and as required by law, we are aware of the significant variability among workers' compensation and similar laws, and include this provision to ensure that existing workers' compensation systems are not disrupted by this rule. We note that the minimum necessary standard applies to disclosures under this paragraph.

Under this provision, a covered entity may disclose protected health information regarding an individual to a party responsible for payment of workers' compensation benefits to the individual, and to an agency responsible for administering and/or adjudicating the individual's claim for workers' compensation benefits. For purposes of this paragraph, workers' compensation benefits include benefits under programs such as the Black Lung Benefits Act, the federal Employees' Compensation Act, the Longshore and Harbor Workers' Compensation Act, and the Energy Employees' Occupational Illness Compensation Program Act.

Additional Considerations

We have included a general authorization for disclosures under workers' compensation systems to be consistent with the intent of Congress, which defined workers' compensation carriers as excepted benefits under HIPAA. We recognize that there are significant privacy issues raised by how individually identifiable health information is used and disclosed in workers' compensation systems, and believe that states or the federal government should enact standards that address those concerns.

Section 164.514—Other Procedural Requirements Relating To Uses and Disclosures of Protected Health Information

Section 164.514(a)–(c)—De-identification

In § 164.506(d) of the NPRM, we proposed that the privacy standards would apply to ''individually identifiable health information,'' and not to information that does not identify the subject individual. The statute defines individually identifiable health information as certain health information:

(i) Which identifies the individual, or

(ii) With respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

As we pointed out in the NPRM, difficulties arise because, even after removing obvious identifiers (*e.g.,* name, social security number, address), there is always some probability or risk that any information about an individual can be attributed to that individual.

The NPRM proposed two alternative methods for determining when sufficient identifying information has been removed from a record to render the information de-identified and thus not subject to the rule. First, the NPRM proposed the establishment of a ''safe harbor'': if all of a list of 19 specified items of information had been removed, and the covered entity had no reason to believe that the remaining information could be used to identify the subject of the information (alone or in combination with other information), the covered entity would have been presumed to have created de-identified information. Second, the NPRM proposed an alternative method so that covered entities with sufficient statistical experience and expertise could remove or encrypt a combination of information different from the enumerated list, using commonly accepted scientific and statistical standards for disclosure avoidance. Such covered entities would have been able to include information from the enumerated list of 19 items if they (1) believed that the probability of re-identification was very low, and (2) removed additional information if they had a reasonable basis to believe that the resulting information could be used to re-identify someone.

We proposed that covered entities and their business partners be permitted to use protected health information to create de-identified health information using either of these two methods. Covered entities would have been permitted to further use and disclose such de-identified information in any way, provided that they did not disclose the key or other mechanism that would have enabled the information to be re-identified, and provided that they reasonably believed that such use or disclosure of de-identified information would not have resulted in the use or

disclosure of protected health information.

A number of examples were provided of how valuable such de-identified information would be for various purposes. We expressed the hope that covered entities, their business partners, and others would make greater use of de-identified health information than they do today, when it is sufficient for the purpose, and that such practice would reduce the burden and the confidentiality concerns that result from the use of individually identifiable health information for some of these purposes.

In §§ 164.514(a)-(c) of this final rule, we make several modifications to the provisions for de-identification. First, we explicitly adopt the statutory standard as the basic regulatory standard for whether health information is individually identifiable health information under this rule. Information is not individually identifiable under this rule if it does not identify the individual, or if the covered entity has no reasonable basis to believe it can be used to identify the individual. Second, in the implementation specifications we reformulate the two ways in which a covered entity can demonstrate that it has met the standard.

One way a covered entity may demonstrate that it has met the standard is if a person with appropriate knowledge and experience applying generally accepted statistical and scientific principles and methods for rendering information not individually identifiable makes a determination that the risk is very small that the information could be used, either by itself or in combination with other available information, by anticipated recipients to identify a subject of the information. The covered entity must also document the analysis and results that justify the determination. We provide guidance regarding this standard in our responses to the comments we received on this provision.

We also include an alternate, safe harbor, method by which covered entities can demonstrate compliance with the standard. Under the safe harbor, a covered entity is considered to have met the standard if it has removed all of a list of enumerated identifiers, and if the covered entity has no actual knowledge that the information could be used alone or in combination to identify a subject of the information. We note that in the NPRM, we had proposed that to meet the safe harbor, a covered entity must have ''no reason to believe'' that the information remained identifiable after the enumerated identifiers were removed. In the final rule, we have changed the standard to one of actual knowledge in order to provide greater certainty to covered entities using the safe harbor approach.

In the safe harbor, we explicitly allow age and some geographic location information to be included in the de-identified information, but all dates directly related to the subject of the information must be removed or limited to the year, and zip codes must be removed or aggregated (in the form of most 3-digit zip codes) to include at least 20,000 people. Extreme ages of 90 and over must be aggregated to a category of 90+ to avoid identification of very old individuals. Other demographic information, such as gender, race, ethnicity, and marital status are not included in the list of identifiers that must be removed.

The intent of the safe harbor is to provide a means to produce some de-identified information that could be used for many purposes with a very small risk of privacy violation. The safe harbor is intended to involve a minimum of burden and convey a maximum of certainty that the rules have been met by interpreting the statutory ''reasonable basis to believe that the information can be used to identify the individual'' to produce an easily followed, cook book approach.

Covered entities may use codes and similar means of marking records so that they may be linked or later re-identified, if the code does not contain information about the subject of the information (for example, the code may not be a derivative of the individual's social security number), and if the covered entity does not use or disclose the code for any other purpose. The covered entity is also prohibited from disclosing the mechanism for re-identification, such as tables, algorithms, or other tools that could be used to link the code with the subject of the information.

Language to clarify that covered entities may contract with business associates to perform the de-identification has been added to the section on business associates.

Section 164.514(d)—Minimum Necessary

The proposed rule required a covered entity to make all reasonable efforts not to use or disclose more than the minimum amount of protected health information necessary to accomplish the intended purpose of the use or disclosure (proposed § 164.506(b)).

The proposed minimum necessary standard did not apply to uses or disclosures that were made by covered entities at the request of the individual, either to allow the individual access to protected health information about him or her or pursuant to an authorization initiated by the individual. The requirement also did not apply to uses and disclosures made: pursuant to the compliance and enforcement provisions of the rule; as required by law and permitted by the regulation without individual authorization; by a covered health care provider to a health plan, when the information was requested for audit and related purposes. Finally, the standard did not apply to the HIPAA administrative simplification transactions.

The proposed implementation specifications would have required a covered entity to have procedures to: (i) Identify appropriate persons within the entity to determine what information should be used or disclosed consistent with the minimum necessary standard; (ii) ensure that those persons make the minimum necessary determinations, when required; and (iii) within the limits of the entity's technological capabilities, provide for the making of such determinations individually. The proposal allowed a covered entity, when making disclosures to public officials that were permitted without individual authorization but not required by other law, to reasonably rely on the representations of such officials that the information requested was the minimum necessary for the stated purpose(s).

The preamble provided further guidance. The preamble explained that covered entities could not have general policies of approving all requests (or all requests of a particular type) without carefully considering certain criteria (see ''Criteria,'' below) as well as other information specific to the request. The minimum necessary determination would have needed to be consistent with and directly related to the purpose of the use or disclosure. Where there was ambiguity regarding the information to be used or disclosed, the preamble directed covered entities to interpret the ''minimum necessary'' standard to ''require'' the covered entity to make some effort to limit the amount of protected health information used/disclosed.

The proposal would have required the minimum necessary determination to take into consideration the ability of a covered entity to delimit the amount of information used or disclosed. The preamble noted that these determinations would have to be made under a reasonableness standard: covered entities would be required to make reasonable efforts and to incur reasonable expense to limit the use or

disclosure. The ''reasonableness'' of limiting particular uses or disclosures was to be determined based on the following factors (which were not included in the regulatory text):

a. The extent to which the use or disclosure would extend the number of persons with access to the protected health information.

b. The likelihood that further uses or disclosures of the protected health information could occur.

c. The amount of protected health information that would be used or disclosed.

d. The importance of the use or disclosure.

e. The potential to achieve substantially the same purpose with de-identified information. For disclosures, each covered entity would have been required to have policies for determining when protected health information must be stripped of identifiers.

f. The technology available to limit the amount of protected health information used/disclosed.

g. The cost of limiting the use/disclosure.

h. Any other factors that the covered entity believed were relevant to the determination.

The proposal shifted the ''minimum necessary'' burden off of covered providers when they were being audited by a health plan. The preamble explained that the duty would have been shifted to the payor to request the minimum necessary information for the audit purpose, although the regulatory text did not include such a requirement. Outside of the audit context, the preamble stated that a health plan would be required, when requesting a disclosure, to limit its requests to the information required to achieve the purpose of the request; the regulation text did not include this requirement.

The preamble stated that disclosure of an entire medical record, in response to a request for something other than the entire medical record, would presumptively violate the minimum necessary standard.

This final rule significantly modifies the proposed requirements for implementing the minimum necessary standard. For all uses and many disclosures and requests for disclosures from other covered entities, we require covered entities to implement policies and procedures for ''minimum necessary'' uses and disclosures. Implementation of such policies and procedures is required in lieu of making the ''minimum necessary'' determination for each separate use or disclosure as discussed in the proposal. Disclosures to or requests by a health care provider for treatment purposes are not subject to the standard (see § 164.502).

Specifically (and as further described below), the proposed requirement for individual review of all uses of protected health information is replaced with a requirement for covered entities to implement policies and procedures that restrict access and uses based on the specific roles of members of the covered entity's workforce. Routine disclosures also are not subject to individual review; instead, covered entities must implement policies and procedures to limit the protected health information in routine disclosures to the minimum necessary to achieve the purpose of that type of disclosure. The proposed exclusion of disclosures to health plans for audit purposes is deleted and replaced with a general requirement that covered entities must limit requests to other covered entities for individually identifiable health information to what is reasonably necessary for the use or disclosure intended. The other exclusions from the standard are unchanged from the proposed rule (*e.g.,* for individuals' access to information about themselves, pursuant to an authorization initiated by the individual, for enforcement of this rule, as required by law).

The language of the basic ''standard'' itself is largely unchanged; covered entities must make reasonable efforts to use or disclose or to request from another covered entity, only the minimum amount of protected health information required to achieve the purpose of a particular use or disclosure. We delete the word ''all'' from the ''reasonable efforts'' that covered entities must take in making a ''minimum necessary'' determination. The implementation specifications are significantly modified, and differ based on whether the activity is a use or disclosure.

Similarly, a ''minimum necessary'' disclosure for oversight purposes in accordance with § 164.512(d) could include large numbers of records to allow oversight agencies to perform statistical analyses to identify deviations in payment or billing patterns, and other data analyses.

Uses of Protected Health Information

A covered entity must implement policies and procedures to identify the persons or classes of persons in the entity's workforce who need access to protected health information to carry out their duties, the category or categories of protected health information to which such persons or classes need access, and the conditions, as appropriate, that would apply to such access. Covered entities must also implement policies and procedures to limit access to only the identified persons, and only to the identified protected health information. The policies and procedures must be based on reasonable determinations regarding the persons or classes of persons who require protected health information, and the nature of the health information they require, consistent with their job responsibilities.

For example, a hospital could implement a policy that permitted nurses access to all protected health information of patients in their ward while they are on duty. A health plan could permit its underwriting analysts unrestricted access to aggregate claims information for rate setting purposes, but require documented approval from its department manager to obtain specific identifiable claims records of a member for the purpose of determining the cause of unexpected claims that could influence renewal premium rate setting.

The ''minimum necessary'' standard is intended to reflect and be consistent with, not override, professional judgment and standards. For example, we expect that covered entities will implement policies that allow persons involved in treatment to have access to the entire record, as needed.

Disclosures of Protected Health Information

For any type of disclosure that is made on a routine, recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that permit only the disclosure of the minimum protected health information reasonably necessary to achieve the purpose of the disclosure. Individual review of each disclosure is not required. Instead, under § 164.514(d)(3), these policies and procedures must identify the types of protected health information to be disclosed, the types of persons who would receive the protected health information, and the conditions that would apply for such access. We recognize that specific disclosures within a type may vary, and require that the policies address what is the norm for the type of disclosure involved. For example, a covered entity may decide to participate in research studies and therefore establish a protocol to minimize the information released for such purposes, *e.g.,* by requiring researchers requesting disclosure of data contained in paper-based records to review the paper records on-site and to

abstract only the information relevant to the research. Covered entities must develop policies and procedures (which may be standard protocols) to apply to disclosures to routinely hired types of business associates. For instance, a standard protocol could describe the subset of information that may be disclosed to medical transcription services.

For non-routine disclosures, a covered entity must develop reasonable criteria for determining, and limiting disclosure to, only the minimum amount of protected health information necessary to accomplish the purpose of the disclosure. They also must establish and implement procedures for reviewing such requests for disclosures on an individual basis in accordance with these criteria.

Disclosures to health care providers for treatment purposes are not subject to these requirements.

Covered entities' policies and procedures must provide that disclosure of an entire medical record will not be made except pursuant to policies which specifically justify why the entire medical record is needed. For instance, disclosure of all protected health information to an accreditation group would not necessarily violate the regulation, because the entire record may be the ''minimum necessary'' for its purpose; covered entities may establish policies allowing for and justifying such a disclosure. Disclosure of the entire medical record absent such documented justification is a presumptive violation of this rule.

Requests for Protected Health Information

For requests for protected health information from other covered entities made on a routine, recurring basis, the requesting covered entities' policies and procedures may establish standard protocols describing what information is reasonably necessary for the purposes and limiting their requests to only that information, in lieu of making this determination individually for each request. For all other requests, the policies and procedures must provide for review of the requests on an individualized basis. A request by a covered entity may be made in order to obtain information that will subsequently be disclosed to a third party, for example, to obtain information that will then be disclosed to a business associate for quality assessment purposes; such requests are subject to this requirement.

Covered entities' policies and procedures must provide that requests for an entire medical record will not be made except pursuant to policies which specifically justify why the entire medical record is needed. For instance, a health plan's request for all protected health information from an applicant for insurance would not necessarily violate the regulation, because the entire record may be the ''minimum necessary'' for its purpose. Covered entities may establish policies allowing for and justifying such a request. A request for the entire medical record absent such documented justification is a presumptive violation of this rule.

Reasonable Reliance

A covered entity may reasonably rely on the assertion of a requesting covered entity that it is requesting the minimum protected health information necessary for the stated purpose. A covered entity may also rely on the assertions of a professional (such as attorneys and accountants) who is a member of its workforce or its business associate regarding what protected health information he or she needs in order to provide professional services to the covered entity when such person represents that the information requested is the minimum necessary. As we proposed in the NPRM, covered entities making disclosures to public officials that are permitted under § 164.512 may rely on the representation of a public official that the information requested is the minimum necessary.

Uses and Disclosures for Research

In making a minimum necessary determination regarding the use or disclosure of protected health information for research purposes, a covered entity may reasonably rely on documentation from an IRB or privacy board describing the protected health information needed for research and consistent with the requirements of § 164.512(i), ''Uses and Disclosures for Research Purposes.'' A covered entity may also reasonably rely on a representation made by the requestor that the information is necessary to prepare a research protocol or for research on decedents. The covered entity must ensure that the representation or documentation of IRB or privacy board approval it obtains from a researcher describes with sufficient specificity the protected health information necessary for the research. Covered entities must use or disclose such protected health information in a manner that minimizes the scope of the use or disclosure.

Standards for Electronic Transactions

We clarify that under § 164.502(b)(2)(v), covered entities are not required to apply the minimum necessary standard to the required or situational data elements specified in the implementation guides for HIPAA administrative simplification standard transactions in the Transactions Rule. The standard does apply for uses or disclosures in standard transactions that are made at the option of the covered entity.

Section 164.514(e)—Marketing

In the proposed rule, we would have required covered entities to obtain the individual's authorization in order to use or disclose protected health information to market health and non-health items and services.

We have made a number of changes in the final rule that relate to marketing. In the final rule, we retain the general rule that covered entities must obtain the individual's authorization before making uses or disclosures of protected health information for marketing. However, we add a new definition of ''marketing'' that clarifies that certain activities, such as communications made by a covered entity for the purpose of describing the products and services it provides, are not marketing. See § 164.501 and the associated preamble regarding the definition of marketing. In the final rule we also permit covered entities to use and disclose protected health information for certain marketing activities without individual authorization, subject to conditions enumerated at § 164.514(e).

First, § 164.514(e) permits a covered entity to use or disclose protected health information without individual authorization to make a marketing communication if the communication occurs in a face-to-face encounter with the individual. This provision would permit a covered entity to discuss any services and products, including those of a third-party, without restriction during a face-to-face communication. A covered entity also could give the individual sample products or other information in this setting.

Second, we permit a covered entity to use or disclose protected health information without individual authorization to make marketing communications involving products or services of only nominal value. This provision ensures that covered entities do not violate the rule when they distribute calendars, pens and other merchandise that generally promotes the covered entity.

Third, we permit a covered entity to use or disclose protected health information without individual authorization to make marketing communications about the health-

related products or services of the covered entity or of a third party if the communication: (1) Identifies the covered entity as the party making the communication; (2) to the extent that the covered entity receives direct or indirect remuneration from a third-party for making the communication, prominently states that fact; (3) except in the case of a general communication (such as a newsletter), contains instructions describing how the individual may opt-out of receiving future communications about health-related products and services; and (4) where protected health information is used to target the communication about a product or service to individuals based on their health status or health condition, explains why the individual has been targeted and how the product or service relates to the health of the individual. The final rule also requires a covered entity to make a determination, prior to using or disclosing protected health information to target a communication to individuals based on their health status or condition, that the product or service may be beneficial to the health of the type or class of individual targeted to receive the communication.

This third provision accommodates the needs of health care entities to be able to discuss their own health-related products and services, or those of third parties, as part of their everyday business and as part of promoting the health of their patients and enrollees. The provision is restricted to uses by covered entities or disclosures to their business associates pursuant to a contract that requires confidentiality, ensuring that protected health information is not distributed to third parties. To provide individuals with a better understanding of how their protected health information is being used for marketing, the provision requires that the communication identify that the covered entity is the source of the communication; a covered entity may not send out information about the product of a third party without disclosing to the individual where the communication originated. We also require covered entities to disclose any direct or indirect remuneration from third parties. This requirement permits individuals to better understand why they are receiving a communication, and to weigh the extent to which their information is being used to promote their health or to enrich the covered entity. Covered entities also are required to include in their communication (unless it is a general newsletter or similar device) how the individual may prevent further communications about health-related products and services. This provision enhances individuals' control over how their information is being used. Finally, where a covered entity targets communications to individuals on the basis of their health status or condition, we require that the entity make a determination that the product or service being communicated may be beneficial to the health of the type of individuals targeted, and that the communication to the targeted individuals explain why they have been targeted and how the product or service relates to their health. This final provision balances the advantages that accrue from health care entities informing their patients and enrollees of new or valuable health products with individuals' expectations that their protected health information will be used to promote their health.

Section 164.514(f)—Fundraising

We proposed in the NPRM to require covered entities to obtain authorization from an individual in order to use the individual's protected health information for fundraising activities.

As noted in § 164.501, in the final rule we define fundraising on behalf of a covered entity to be a health care operation. In § 164.514, we permit a covered entity to use protected health information without individual authorization for fundraising on behalf of itself, provided that it limits the information that it uses to demographic information about the individual and the dates that it has provided service to the individual (see the § 164.501 discussion of ''health care operations''). In addition, we require fundraising materials to explain how the individual may opt out of any further fundraising communications, and covered entities are required to honor such requests. We permit a covered entity to disclose the limited protected health information to a business associate for fundraising on its own behalf. We also permit a covered entity to disclose the information to an institutionally related foundation.

By ''institutionally related foundation,'' we mean a foundation that qualifies as a nonprofit charitable foundation under section 501(c)(3) of the Internal Revenue Code and that has in its charter statement of charitable purposes an explicit linkage to the covered entity. An institutionally related foundation may, as explicitly stated in its charter, support the covered entity as well as other covered entities or health care providers in its community. For example, a covered hospital may disclose for fundraising on its own behalf the specified protected health information to a nonprofit foundation established for the specific purpose of raising funds for the hospital or to a foundation that has as its mission the support of the members of a particular hospital chain that includes the covered hospital. The term does not include an organization with a general charitable purpose, such as to support research about or to provide treatment for certain diseases, that may give money to a covered entity, because its charitable purpose is not specific to the covered entity.

Section 164.514(g)—Underwriting

As described under the definition of ''health care operations'' (§ 164.501), protected health information may be used or disclosed for underwriting and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits. This final rule includes a requirement, not included in the NPRM, that health plans receiving such information for these purposes may not use or disclose it for any other purpose, except as may be required by law, if the insurance or benefits contract is not placed with the health plan.

Section 164.514(h)—Verification of Identity and Authority of Persons Requesting Protected Health Information

Disclosure of Protected Health Information

We reorganize the provision regarding verification of identity of individuals requesting protected health information to improve clarity, but we retain the substance of requirements proposed in the NPRM in § 164.518(c), as follows.

The covered entity must establish and use written policies and procedures (which may be standard protocols) that are reasonably designed to verify the identity and authority of the requestor where the covered entity does not know the person requesting the protected health information. The knowledge of the person may take the form of a known place of business, address, phone or fax number, as well a known human being. Where documentation, statements or representations, whether oral or written, from the person requesting the protected health information is a condition of disclosure under this rule or other law, this verification must involve obtaining such documentation statement, or representation. In such a case, additional verification is only required where this regulation (or other law)

requires additional proof of authority and identity.

The NPRM proposed that covered entities would be permitted to rely on the required documentation of IRB or privacy board approval to constitute sufficient verification that the person making the request was a researcher and that the research is authorized. The final rule retains this provision.

For most disclosures, verifying the authority for the request means taking reasonable steps to verify that the request is lawful under this regulation. Additional proof is required by other provisions of this regulation where the request is made pursuant to § 164.512 for national priority purposes. Where the person requesting the protected health information is a public official, covered entities must verify the identity of the requester by examination of reasonable evidence, such as a written statement of identity on agency letterhead, an identification badge, or similar proof of official status. Similarly, covered entities are required to verify the legal authority supporting the request by examination of reasonable evidence, such as a written request provided on agency letterhead that describes the legal authority for requesting the release. Where § 164.512 explicitly requires written evidence of legal process or other authority before a disclosure may be made, a public official's proof of identity and the official's oral statement that the request is authorized by law are not sufficient to constitute the required reasonable evidence of legal authority; under these provisions, only the required written evidence will suffice.

In some circumstances, a person or entity acting on behalf of a government agency may make a request for disclosure of protected health information under these subsections. For example, public health agencies may contract with a nonprofit agency to collect and analyze certain data. In such cases, the covered entity is required to verify the requestor's identity and authority through examination of reasonable documentation that the requestor is acting on behalf of the government agency. Reasonable evidence includes a written request provided on agency letterhead that describes the legal authority for requesting the release and states that the person or entity is acting under the agency's authority, or other documentation, including a contract, a memorandum of understanding, or purchase order that confirms that the requestor is acting on behalf of the government agency.

In some circumstances, identity or authority will be verified as part of meeting the underlying requirements for disclosure. For example, a disclosure under § 164.512(j)(1)(i) to avert an imminent threat to safety is lawful only if made in the good faith belief that the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public, and to a person reasonably able to prevent or lessen the threat. If these conditions are met, no further verification is needed. In such emergencies, the covered entity is not required to demand written proof that the person requesting the protected health information is legally authorized. Reasonable reliance on verbal representations are appropriate in such situations.

Similarly, disclosures permitted under § 164.510(a) for facility directories may be made to the general public; the covered entity's policies and procedures do not need to address verifying the identity and authority for these disclosures. In § 164.510(b) we do not require verification of identity for persons assisting in an individual's care or for notification purposes. For disclosures when the individual is not present, such as when a friend is picking up a prescription, we allow the covered entity to use professional judgment and experience with common practice to make reasonable inferences.

Under § 164.524, a covered entity is required to give individuals access to protected health information about them (under most circumstances). Under the general verification requirements of § 164.514(h), the covered entity is required to take reasonable steps to verify the identity of the individual making the request. We do not mandate particular identification requirements (*e.g.,* drivers licence, photo ID), but rather leave this to the discretion of the covered entity. The covered entity must also establish and document procedures for verification of identity and authority of personal representatives, if not known to the entity. For example, a health care provider can require a copy of a power of attorney, or can ask questions to determine that an adult acting for a young child has the requisite relationship to the child.

In Subpart C of Part 160, we require disclosure to the Secretary for purposes of enforcing this regulation. When a covered entity is asked by the Secretary to disclose protected health information for compliance purposes, the covered entity must verify the same information that it is required to verify for any other law enforcement or oversight request for disclosure.

Use of Protected Health Information

The proposed rule's verification requirements applied to any person requesting protected health information, whether for a use or a disclosure. In the final regulation, the verification provisions apply only to disclosures of protected health information. The requirements in § 164.514(d), for implementation of policies and procedures for ''minimum necessary'' uses of protected health information, are sufficient to ensure that only appropriate persons within a covered entity will have access to protected health information.

Section 164.520—Notice of Privacy Practices for Protected Health Information

Section 164.520(a)—Right to Notice

We proposed to establish a right for individuals to receive adequate notice of how covered health care providers and health plans use and disclose protected health information, and of the individual's rights with respect to that information.

In the final regulation, we retain the general right for individuals to receive and the requirement for covered entities to produce a notice of privacy practices, with significant modifications to the content and distribution requirements.

We also modify the requirements with respect to certain covered entities. First, in § 164.500(b)(2), we clarify that a health care clearinghouse that creates or receives protected health information other than as a business associate of a covered entity must produce a notice. If a health care clearinghouse creates or receives protected health information only as a business associate of other covered entities, it is not required to produce a notice.

Second, in § 164.520(a)(2), we clarify the notice requirements with respect to group health plans. Individuals who receive health benefits under a group health plan other than through insurance are entitled to a notice from the group health plan; self-insured group health plans must maintain a notice that meets the requirements of this section and must provide the notice in accordance with the requirements of § 164.520(c). At a minimum, the self-insured group health plan's notice must describe the group health plan's privacy practices with respect to the protected health information it creates or receives through its self-insured arrangements. For example, if a group health plan maintains both fully-insured and self-insured arrangements, the group health plan must, at a minimum, maintain and provide a notice that describes its

privacy practices with respect to protected health information it creates or receives through the self-insured arrangements. This notice would be distributed to all participants in the self-insured arrangements (in accordance with § 164.520(c)(1)) and would also be available on request to other persons, including participants in the fully-insured arrangements.

Individuals who receive health benefits under a group health plan through an insurance contract (i.e., a fully-insured group health plan) are entitled to a notice from the issuer or HMO through which they receive their health benefits. The health insurance issuer or HMO must maintain and provide the notice in accordance with § 164.520(c)(1). In addition, some fully-insured group health plans are required to maintain and provide a notice of the group health plan's privacy practices. If a group health plan provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and the group health plan creates or receives protected health information in addition to summary information (as defined in § 164.504(a)) and information about individuals' enrollment in or disenrollment from a health insurance issuer or HMO offered by the group health plan, the group health plan must maintain a notice that meets the requirements of this section and must provide the notice upon request of any person. The group health plan is not required to meet the other distribution requirements of § 164.520(c)(1). Individuals enrolled in such group health plans have the right to notice of the health insurance issuer or HMO's privacy practices and, on request, to notice of the group health plan's privacy practices. If the group health plan, however, provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and the only protected health information the group health plan creates or receives is summary information (as defined in § 164.504(a)) and information about individuals' enrollment in or disenrollment from a health insurance issuer or HMO offered by the group health plan, the group health plan is not required to maintain or provide a notice under this section. In this case, the individuals enrolled in the group health plan would receive notice of the health insurance issuer or HMO's privacy practices, but would not be entitled to notice of the group health plan's privacy practices.

Third, in § 164.520(a)(3), we clarify that inmates do not have a right to notice under this section and a correctional institution that is a covered entity is not required to produce a notice. No person, including a current or former inmate, has the right to notice of such a covered entity's privacy practices.

Section 164.520(b)—Content of Notice

We proposed to require the notice to be written in plain language and contain each of the following elements: a description of the uses and disclosures expected to be made without individual authorization; statements that other uses and disclosures would be made only with the individual's authorization and that the individual could revoke such authorization; descriptions of the rights to request restrictions, inspect and copy protected health information, amend or correct protected health information, and receive an accounting of disclosures of protected health information; statements about the entity's legal requirements to protect privacy, provide notice, and adhere to the notice; a statement about how individuals would be informed of changes to the entity's policies and procedures; instructions on how to make complaints with the entity or Secretary; the name and telephone number of a contact person or office; and the date the notice was produced. We provided a model notice of information policies and procedures for covered health care providers.

In § 164.520(b), and immediately below in this preamble, we describe the notice content requirements for the final rule. As described in detail, below, we make substantial changes to the uses and disclosures of protected health information that must be described in the notice. Unlike the proposed rule, we do not include a model notice. We intend to develop further guidance on notice requirements prior to the compliance date of this rule. In this section of the final rule, we also refer to the covered entity's privacy ''practices,'' rather than its ''policies and procedures.'' The purpose of this change in vocabulary is to clarify that a covered entity's ''policies and procedures'' is a detailed documentation of all of the entity's privacy practices as required under this rule, not just those described in the notice. For example, we require covered entities to have policies and procedures implementing the requirements for ''minimum necessary'' uses and disclosures of protected health information, but these policies and procedures need not be reflected in the entity's notice. Similarly, we require covered entities to have policies and procedures for assuring individuals access to protected health information about them. While such policies and procedures will need to include documentation of the designated record sets subject to access, who is authorized to determine when information will be withheld from an individual, and similar details, the notice need only explain generally that individuals have the right to inspect and copy information about them, and tell individuals how to exercise that right.

A covered entity that adopts and follows the notice content and distribution requirements described below will have provided adequate notice. However, the requirements for the content of the notice are not intended to be exclusive. As with the rest of the rule, we specify minimum requirements, not best practices. Covered entities may want to include more detail. We note that all federal agencies must still comply with the Privacy Act of 1974. This means that federal agencies that are covered entities or have covered health care components must comply with the notice requirements of the Privacy Act as well as those included in this rule.

In addition, covered entities may want or be required to produce more than one notice in order to satisfy the notice content requirements under this rule. For example, a covered entity that conducts business in multiple states with different laws regarding the uses and disclosures that the covered entity is permitted to make without authorization may be required to produce a different notice for each state. A covered entity that conducts business both as part of an organized health care arrangement or affiliated covered entity and as an independent enterprise (e.g., a physician who sees patients through an on-call arrangement with a hospital and through an independent private practice) may want to adopt different privacy practices with respect to each line of business; such a covered entity would be required to produce a different notice describing the practices for each line of business. Covered entities must produce notices that accurately describe the privacy practices that are relevant to the individuals receiving the notice.

Required Elements

Plain Language

As in the proposed rule, we require the notice to be written in plain language. A covered entity can satisfy the plain language requirement if it makes a reasonable effort to: organize material to serve the needs of the reader; write short sentences in the active voice, using ''you'' and other pronouns; use common, everyday words in sentences; and divide material into short sections.

We do not require particular formatting specifications, such as easy-to-read design features (e.g., lists, tables, graphics, contrasting colors, and white space), type face, and font size. However, the purpose of the notice is to inform the recipients about their rights and how protected health information collected about them may be used or disclosed. Recipients who cannot understand the covered entity's notice will miss important information about their rights under this rule and about how the covered entity is protecting health information about them. One of the goals of this rule is to create an environment of open communication and transparency with respect to the use and disclosure of protected health information. A lack of clarity in the notice could undermine this goal and create misunderstandings. Covered entities have an incentive to make their notice statements clear and concise. We believe that the more understandable the notice is, the more confidence the public will have in the covered entity's commitment to protecting the privacy of health information.

It is important that the content of the notice be communicated to all recipients and therefore we encourage the covered entity to consider alternative means of communicating with certain populations. We note that any covered entity that is a recipient of federal financial assistance is generally obligated under Title VI of the Civil Rights Act of 1964 to provide material ordinarily distributed to the public in the primary languages of persons with limited English proficiency in the recipients' service areas. Specifically, this Title VI obligation provides that, where a significant number or proportion of the population eligible to be served or likely to be directly affected by a federally assisted program needs service or information in a language other than English in order to be effectively informed of or participate in the program, the recipient shall take reasonable steps, considering the scope of the program and the size and concentration of such population, to provide information in languages appropriate to such persons. For covered entities not subject to Title VI, the Title VI standards provide helpful guidance for effectively communicating the content of their notices to non-English speaking populations.

We also encourage covered entities to be attentive to the needs of individuals who cannot read. For example, an employee of the covered entity could read the notice to individuals upon request or the notice could be incorporated into a video presentation that is played in the waiting area.

Header

Unlike the proposed rule, covered entities must include prominent and specific language in the notice that indicates the importance of the notice. This is the only specific language we require covered entities to include in the notice. The header must read, ''THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.''

Uses and Disclosures

We proposed to require covered entities to describe in plain language the uses and disclosures of protected health information, and the covered entity's policies and procedures with respect to such uses and disclosures, that the health plan or covered provider expected to make without individual authorization. The covered provider or health plan would have had to distinguish between those uses and disclosures required by law and those permitted but not required by law.

We also proposed to require covered health care providers and health plans to state in the notice that all other uses and disclosures would be made only with the individual's authorization and that such authorization could be revoked. The notice would also have been required to state that the individual could request restrictions on certain uses and disclosures and that the covered entity would not be required to agree to such a request.

We significantly modify these requirements in the final rule. Covered entities must describe all uses and disclosures of protected health information that they are permitted or required to make under this rule without authorization, including those uses and disclosures subject to the consent requirements under § 164.506. If other applicable law prohibits or materially limits the covered entity's ability to make any uses or disclosures that would otherwise be permitted under the rule, the covered entity must describe only the uses and disclosures permitted under the more stringent law.

Covered entities must separately describe each purpose for which they are permitted to use or disclose protected health information under this rule without authorization, and must do so in sufficient detail to place the individual on notice of those uses and disclosures. With respect to uses and disclosures to carry out treatment, payment, and health care operations, the description must include at least one example of the types of uses and disclosures that the covered entity is permitted to make. This requirement is intended to inform individuals of all the uses and disclosures that the covered entity is legally required or permitted to make under applicable law, even if the covered entity does not anticipate actually making such uses and disclosures. We do not require covered entities to distinguish in their notices between those uses and disclosures required by law and those permitted but not required by law.

Unlike the proposed rule, we additionally require covered entities that wish to contact individuals for any of the following activities to list these activities in the notice: providing appointment reminders, describing or recommending treatment alternatives, providing information about health-related benefits and services that may be of interest to the individual, or soliciting funds to benefit the covered entity. If the covered entity does not include these statements in its notice, it is prohibited from using or disclosing protected health information for these activities without authorization. See § 164.502(i).

In addition, if a group health plan, or a health insurance issuer or HMO with respect to a group health plan, wants the option to disclose protected health information to a group health plan sponsor without authorization as permitted under § 164.504(f), the group health plan, health insurance issuer or HMO must describe that practice in its notice.

As in the proposed rule, the notice must state that all other uses and disclosures will be made only with the individual's authorization and that the individual has the right to revoke such authorization.

We anticipate this requirement will lead to significant standardization of the notice. This language could be the same for every covered entity of a particular type within a state, territory, or other locale. We encourage states, state professional associations, and other organizations to develop model language to assist covered entities in preparing their notices.

Individual Rights

As in the proposed rule, covered entities must describe individuals' rights under the rule and how individuals may exercise those rights with respect to the covered entity. Covered entities must describe each of the following rights, as provided under the rule: the right to request restrictions

on certain uses and disclosures, including a statement that the covered entity is not required to agree to a requested restriction (§ 164.522(a)); the right to receive confidential communications of protected health information (§ 164.522(b)); the right to inspect and copy protected health information (§ 164.524); the right to amend protected health information (§ 164.526); and the right to an accounting of disclosures of protected health information (§ 164.528). We additionally require the notice to describe the right of an individual, including an individual that has agreed to receive the notice electronically, to obtain a paper copy of the notice upon request.

Covered Entity's Duties

As in the proposed rule, covered entities must state in the notice that they are required by law to maintain the privacy of protected health information, to provide a notice of their legal duties and privacy practices, and to abide by the terms of the notice currently in effect. In the final rule, we additionally require the covered entity, if it wishes to reserve the right to change its privacy practices and apply the revised practices to protected health information previously created or received, to make a statement to that effect and describe how it will provide individuals with a revised notice. (See below for a more detailed discussion of a covered entity's responsibilities when it changes its privacy practices.)

Complaints

As in the proposed rule, a covered entity's notice must inform individuals about how they can lodge complaints with the covered entity if they believe their privacy rights have been violated. See § 164.530(d) and the corresponding preamble discussion for the requirements on covered entities for receiving complaints. The notice must also state that individuals may file complaints with the Secretary. In the final rule, we additionally require the notice to include a statement that the individual will not suffer retaliation for filing a complaint.

Contact

As in the proposed rule, the notice must identify a point of contact where the individual can obtain additional information about any of the matters identified in the notice.

Effective Date

The notice must include the date the notice went into effect, rather than the proposed requirement to include the date the notice was produced. The effective date cannot be earlier than the date on which the notice was first printed or otherwise published. Covered entities may wish to highlight or otherwise emphasize any material modifications that it has made, in order to help the individual recognize such changes.

Optional Elements

As described above, we proposed to require covered entities to describe the uses and disclosures of protected health information that the covered entity in fact expected to make without the individual's authorization. We did not specify any optional elements.

While the final rule requires covered entities to describe all of the types of uses and disclosures permitted or required by law (not just those that the covered entity intends to make), we also permit and encourage covered entities to include optional elements that describe the actual, more limited, uses and disclosures they intend to make without authorization. We anticipate that some covered entities will want to distinguish themselves on the basis of their more stringent privacy practices. For example, covered health care providers who routinely treat patients with particularly sensitive conditions may wish to assure their patients that, even though the law permits them to disclose information for a wide array of purposes, the covered health care provider will only disclose information in very specific circumstances, as required by law, and to avert a serious and imminent threat to health or safety. A covered entity may not include statements in the notice that purport to limit the entity's ability to make uses or disclosures that are required by law or necessary to avert a serious and imminent threat to health or safety.

As described above, if the covered entity wishes to reserve the right to change its privacy practices with respect to the more limited uses and disclosures and apply the revised practices to protected health information previously created or received, it must make a statement to that effect and describe how it will provide individuals with a revised notice. (See below for a more detailed discussion of a covered entity's responsibilities when it changes its privacy practices.)

Revisions to the Notice

We proposed to require a covered entity to adhere to the terms of its notice, and would have permitted it to change its information policies and procedures at any time. We would have required covered health care providers and health plans to update the notice to reflect material changes to the information policies and procedures described in the notice. Changes to the notice would have applied to all protected health information held by the covered entity, including information collected under prior notices. That is, we would not have require covered entities to segregate their records according to the notice in effect at the time the record was created. We proposed to prohibit covered entities from implementing a change to an information policy or procedure described in the notice until the notice was updated to reflect the change, unless a compelling reason existed to make a use or disclosure or take other action that the notice would not have permitted. In these situations, we proposed to require covered entities to document the compelling reason and, within 30 days of the use, disclosure, or other action, change its notice to permit the action.

As in the proposed rule, covered entities are required to adhere to the terms of the notice currently in effect. See § 164.502(i). When a covered entity materially changes any of the uses or disclosures, the individual's rights, the covered entity's legal duties, or other privacy practices described in its notice, it must promptly revise its notice accordingly. See § 164.520(b)(3). (Pursuant to § 164.530(i), it must also revise its policies and procedures.) Except when required by law, a material change to any term in the notice may not be implemented prior to the effective date of the notice in which such material change is reflected. In the final rule, however, we revise the circumstances under and extent to which the covered entity may revise the practices stated in the notice and apply the new practices to protected health information it created or received under prior notice.

Under § 164.530(i), a covered entity that wishes to change its practices over time without segregating its records according to the notice in effect at the time the records were created must reserve the right to do so in its notice. For example, a covered hospital that states in its notice that it will only make public health disclosures required by law, and that does not reserve the right to change this practice, is prohibited from making any discretionary public health disclosures of protected health information created or received during the effective period of that notice. If the covered hospital wishes at some point in the future to make discretionary disclosures for public health purposes, it must revise its notice to so state, and

must segregate its records so that protected health information created or received under the prior notice is not disclosed for discretionary public health purposes. This hospital may then make discretionary public health disclosures of protected health information created or received after the effective date of the revised notice.

If a second covered hospital states in its notice that it will only make public health disclosures required by law, but does reserve the right to change its practices, it is prohibited from making any discretionary public health disclosures of protected health information created or received during the effective period of that notice. If this hospital wishes at some point in the future to make discretionary disclosures for public health purposes, it must revise its notice to so state, but need not segregate its records. As of the effective date of the revised notice, it may disclose any protected health information, including information created or received under the prior notice, for discretionary public health purposes.

Section 164.530(i) and the corresponding discussion in this preamble describes requirements for revision of a covered entity's privacy policies and procedures, including the privacy practices reflected in its notice.

Section 164.520(c)—Provision of Notice

As in the proposed rule, all covered entities that are required to produce a notice must provide the notice upon request of any person. The requestor does not have to be a current patient or enrollee. We intend the notice to be a public document that people can use in choosing between covered entities.

For health plans, we proposed to require health plans to distribute the notice to individuals covered by the health plan as of the compliance date; after the compliance date, at enrollment in the health plan; after enrollment, within 60 days of a material revision to the content of the notice; and no less frequently than once every three years.

As in the proposed rule, under the final rule health plans must provide the notice to all health plan enrollees as of the compliance date. After the compliance date, health plans must provide the notice to all new enrollees at the time of enrollment and to all enrollees within 60 days of a material revision to the notice. Of course, the term ''enrollees'' includes participants and beneficiaries in group health plans.

Unlike the proposed rule, we do not require health plans to distribute the notice every three years. Instead, health plans must notify enrollees no less than once every three years about the availability of the notice and how to obtain a copy.

We also clarify that, in each of these circumstances, if a named insured and one or more dependents are covered by the same policy, the health plan can satisfy the distribution requirement with respect to the dependents by sending a single copy of the notice to the named insured. For example, if an employee of a firm and her three dependents are all covered under a single health plan policy, that health plan can satisfy the initial distribution requirement by sending a single copy of the notice to the employee rather than sending four copies, each addressed to a different member of the family.

We further clarify that if a health plan has more than one notice, it satisfies its distribution requirement by providing the notice that is relevant to the individual or other person requesting the notice. For example, a health insurance issuer may have contracts with two different group health plans. One contract specifies that the issuer may use and disclose protected health information about the participants in the group health plan for research purposes without authorization (subject to the requirements of this rule) and one contract specifies that the issuer must always obtain authorizations for these uses and disclosures. The issuer accordingly develops two notices reflecting these different practices and satisfies its distribution requirements by providing the relevant notice to the relevant group health plan participants.

We proposed to require covered health care providers with face-to-face contact with individuals to provide the notice to all such individuals at the first service delivery to the individual during the one year period after the compliance date. After this one year period, covered providers with face-to-face contact with individuals would have been required to distribute the notice to all new patients at the first service delivery. Covered providers without face-to-face contact with individuals would have been required to provide the notice in a reasonable period of time following first service delivery.

We proposed to require all covered providers to post the notice in a clear and prominent location where it would be reasonable to expect individuals seeking services from the covered provider to be able to read the notice. We would have required revisions to be posted promptly.

In the final rule, we vary the distribution requirements according to whether the covered health care provider has a direct treatment relationship with an individual, rather than whether the covered health care provider has face-to-face contact with an individual. See § 164.501 and the corresponding discussion in this preamble regarding the definition of indirect treatment relationship.

Covered health care providers that have direct treatment relationships with individuals must provide the notice to such individuals as of the first service delivery after the compliance date. This requirement applies whether the first service is delivered electronically or in person. Covered providers may satisfy this requirement by sending the notice to all of their patients at once, by giving the notice to each patient as he or she comes into the provider's office or facility or contacts the provider electronically, or by some combination of these approaches. Covered providers that maintain a physical service delivery site must prominently post the notice where it is reasonable to expect individuals seeking service from the provider to be able to read the notice. The notice must also be available on site for individuals to take on request. In the event of a revision to the notice, the covered provider must promptly post the revision and make it available on site.

Covered health care providers that have indirect treatment relationships with individuals are only required to produce the notice upon request, as described above.

The proposed rule was silent regarding electronic distribution of the notice. Under the final rule, a covered entity that maintains a web site describing the services and benefits it offers must make its privacy notice prominently available through the site.

A covered entity may satisfy the applicable distribution requirements described above by providing the notice to the individual electronically, if the individual agrees to receiving materials from the covered entity electronically and the individual has not withdrawn his or her agreement. If the covered entity knows that the electronic transmission has failed, the covered entity must provide a paper copy of the notice to the individual.

If an individual's first service delivery from a covered provider occurs electronically, the covered provider must provide electronic notice automatically and contemporaneously in response to the individual's first request for service. For example, the first time an individual requests to fill a prescription through a covered internet pharmacy, the pharmacy must automatically and contemporaneously provide the individual with the

pharmacy's notice of privacy practices. An individual that receives a covered entity's notice electronically retains the right to request a paper copy of the notice as described above. This right must be described in the notice.

We note that the Electronic Signatures in Global and National Commerce Act (Pub. L. 106–229) may apply to documents required under this rule to be provided in writing. We do not intend to affect the application of that law to documents required under this rule.

Section 164.520(d)—Joint Notice by Separate Covered Entities

The proposed rule was silent regarding the ability of legally separate covered entities to produce a single notice.

In the final rule, we allow covered entities that participate in an organized health care arrangement to comply with this section by producing a single notice that describes their combined privacy practices. See § 164.501 and the corresponding preamble discussion regarding the definition of organized health care arrangement. (We note that, under § 164.504(d), covered entities that are under common ownership or control may designate themselves as a single affiliated covered entity. Joint notice requirements do not apply to such entities. Single affiliated covered entities must produce a single notice, consistent with the requirements described above for any other covered entity. Covered entities under common ownership or control that elect not to designate themselves as a single affiliated covered entity, however, may elect to produce a joint notice if they meet the definition of an organized health care arrangement.)

The joint notice must meet all of the requirements described above. The covered entities must agree to abide by the terms of the notice with respect to protected health information created or received by the covered entities as part of their participation in the organized health care arrangement. In addition, the joint notice must reasonably identify the covered entities, or class of covered entities, to which the joint notice applies and the service delivery sites, or classes of service delivery sites, to which the joint notice applies. If the covered entities participating in the organized health care arrangement will share protected health information with each other as necessary to carry out treatment, payment, or health care operations relating to the arrangement, that fact must be stated in the notice.

Typical examples where this policy may be useful are health care facilities where physicians and other providers who have offices elsewhere also provide services at the facility (e.g. hospital staff privileges, physicians visiting their patients at a residential facility). In these cases, a single notice may cover both the physician and the facility, if the above conditions are met. The physician is required to have a separate notice covering the privacy practices at the physician's office if those practices are different than the practices described in the joint notice.

If any one of the covered entities included in the joint notice distributes the notice to an individual, as required above, the distribution requirement is met for all of the covered entities included in the joint notice.

Section 164.520(e)—Documentation

As in the proposed rule, we establish documentation requirements for covered entities subject to this provision. In the final rule, we specify that covered entities must retain copies of the notice(s) they issue in accordance with § 164.530(j). See § 164.530(j) and the corresponding preamble discussion for further description of the documentation requirements.

Section 164.522—Rights To Request Privacy Protection for Protected Health Information

Section 164.522(a)—Right of An Individual To Request Restriction of Uses and Disclosures

We proposed that individuals have the right to request that a covered health care provider restrict the use or disclosure of protected health information for treatment, payment, or health care operations. Providers would not have been required to agree to requested restrictions. However, a covered provider that agreed to a restriction could not use or disclose protected health information inconsistent with the restriction. The requirement would not have applied to permissible uses or disclosures under proposed § 164.510, including uses and disclosures in emergency circumstances under proposed § 164.510(k); when the health care services provided were emergency services; or to required disclosures to the Secretary under proposed § 164.522. We would have required covered providers to have procedures for individuals to request restrictions, for agreed-upon restrictions to be documented, for the provider to honor such restrictions, and for notification of the existence of a restriction to others to whom such protected health information is disclosed.

In the final rule, we retain the general right of an individual to request that uses and disclosures of protected health information be restricted and the requirement for covered entities to adhere to restrictions to which they have agreed. However, we include some significant changes and clarifications.

Under the final rule, we extend the right to request restrictions to health plans and to health care clearinghouses that create or receive protected health information other than as a business associate of another covered entity. All covered entities must permit individuals to request that uses and disclosures of protected health information to carry out treatment, payment, and health care operations be restricted and must adhere to restrictions to which they have agreed. A covered entity is not required to agree to a restriction. We note that restrictions between an individual and a covered entity for these or other purposes may be otherwise enforceable under other law.

Under § 164.522(a)(1)(i)(B), the right to request restrictions applies to disclosures to persons assisting in the individual's care under § 164.510(b). An individual may request that a covered entity agree not to disclose protected health information to persons assisting with the individual's care, even if such disclosure is permissible in accordance with § 164.510(b). For example, if an individual requests that a covered entity never disclose protected health information to a particular family member, and the covered entity agrees to that restriction, the covered entity is prohibited from disclosing protected health information to that family member, even if the disclosure would otherwise be permissible under § 164.510(b). We note that individuals additionally have the opportunity to agree or object to disclosures to persons assisting in the individual's care under § 164.510(b)(2). The individual retains the right to agree or object to such disclosures under § 164.510(b)(2), in accordance with the standards of that provision, regardless of whether the individual has requested a restriction under § 164.522(a). See § 164.510(b) and the corresponding preamble discussion regarding the individual's right to agree or object to disclosures to persons assisting in the individual's care.

In §§ 164.522(a)(1)(iii) and (iv) we clarify the requirements with respect to emergency treatment situations. In emergency treatment situations, a covered entity that has agreed to a restriction may use, or disclose to a health care provider, restricted protected health information that is

necessary to provide the emergency treatment. If the covered entity discloses restricted protected health information to a health care provider for emergency treatment purposes, it must request that the provider not further use or disclose the information. We expect covered entities to consider the need for access to protected health information for treatment purposes when considering a request for a restriction, to discuss this need with the individual making the request for restriction, and to agree to restrictions that will not foreseeably impede the individual's treatment. Therefore, we expect covered entities will rarely need to use or disclose restricted protected health information in emergency treatment situations. We do not intend, however, to adversely impact the delivery of health care. We therefore provide a means for the use and disclosure of restricted protected health information in emergency treatment situations, where an unexpected need for the information could arise and there is insufficient time to secure the individual's permission to use or disclose the restricted information.

In § 164.522(a)(1)(v) we clarify that restrictions are not effective under this rule to prevent uses and disclosures required by § 164.502(a)(2)(ii) or permitted under § 164.510(a) (regarding facility directories) or § 164.512 (regarding uses and disclosures for which consent, individual authorization, or opportunity to agree or object is not required). Covered entities are permitted to agree to such restrictions, but if they do so, the restrictions are not enforceable under this rule. For example, a provider who makes a disclosure under § 164.512(j)(1)(i) relating to serious and imminent threats will not be in violation of this rule even if the disclosure is contrary to a restriction agreed to under this paragraph.

In § 164.522(a)(2) we clarify a covered entity's ability to terminate a restriction to which it has agreed. A covered entity may terminate a restriction with the individual's written or oral agreement. If the individual's agreement is obtained orally, the covered entity must document that agreement. A note in the medical record or similar notation is sufficient documentation. If the individual agrees to terminate the restriction, the covered entity may use and disclose protected health information as otherwise permitted under the rule. If the covered entity wants to terminate the restriction without the individual's agreement, it may only terminate the restriction with respect to protected health information it creates or receives after it informs the individual of the termination. The restriction continues to apply to protected health information created or received prior to informing the individual of the termination. That is, any protected health information that had been collected before the termination may not be used or disclosed in a way that is inconsistent with the restriction, but any information that is collected after informing the individual of the termination of the restriction may be used or disclosed as otherwise permitted under the rule.

In § 164.522(a)(3), we clarify that a covered entity must document a restriction to which it has agreed. We do not require a specific form of documentation; a note in the medical record or similar notation is sufficient. The documentation must be retained for six years from the date it was created or the date it was last in effect, whichever is later, in accordance with § 164.530(j).

We eliminate the requirement from the NPRM for covered entities to inform persons to whom they disclose protected health information of the existence of any restriction on that information. A restriction is only binding on the covered entity that agreed to the restriction. We encourage covered entities to inform others of the existence of a restriction when it is appropriate to do so. We note, however, that disclosure of the existence of a restriction often amounts to a de facto disclosure of the restricted information itself. If a restriction does not permit a covered entity to disclose protected health information to a particular person, the covered entity must carefully consider whether disclosing the existence of the restriction to that person would also violate the restriction.

Section 164.522(b)—Confidential Communications Requirements

In the NPRM, we did not directly address the issue of whether an individual could request that a covered entity restrict the manner in which it communicated with the individual. As described above, the NPRM would have provided individuals with the right to request that health care providers restrict uses and disclosures of protected health information for treatment, payment and health care operations, but would not have required providers to agree to such a restriction.

In the final rule, we require covered entities to permit individuals to request that the covered entity provide confidential communications of protected health information about the individual. The requirement applies to communications from the covered entity to the individual, and also communications from the covered entity that would otherwise be sent to the named insured of an insurance policy that covers the individual as a dependent of the named insured. Individuals may request that the covered entity send such communications by alternative means or at alternative locations. For example, an individual who does not want his or her family members to know about a certain treatment may request that the provider communicate with the individual about that treatment at the individual's place of employment, by mail to a designated address, or by phone to a designated phone number. Similarly, an individual may request that the provider send communications in a closed envelope rather than a post card, as an ''alternative means.'' Covered health care providers must accommodate all reasonable requests. Health plans must accommodate all reasonable requests, if the individual clearly states that the disclosure of all or part of the protected health information could endanger the individual. For example, if an individual requests that a health plan send explanations of benefits about particular services to the individual's work rather than home address because the individual is concerned that a member of the individual's household (e.g., the named insured) might read the explanation of benefits and become abusive towards the individual, the health plan must accommodate the request.

The reasonableness of a request made under this paragraph must be determined by a covered entity solely on the basis of the administrative difficulty of complying with the request and as otherwise provided in this section. A covered health care provider or health plan cannot refuse to accommodate a request based on its perception of the merits of the individual's reason for making the request. A covered health care provider may not require the individual to provide a reason for the request as a condition of accommodating the request. As discussed above, a health plan is not required to accommodate a request unless the individual indicates that the disclosure could endanger the individual. If the individual indicates such endangerment, however, the covered entity cannot further consider the individual's reason for making the request in determining whether it must accommodate the request.

A covered health care provider or health plan may refuse to accommodate a request, however, if the individual has

not provided information as to how payment, if applicable, will be handled, or if the individual has not specified an alternative address or method of contact.

Section 164.524—Access of Individuals to Protected Health Information

Section 164.524(a)—Right of Access

In the NPRM, we proposed to establish a right for individuals to access (*i.e.,* inspect and obtain a copy of) protected health information about them maintained by a covered provider or health plan, or its business partners, in a designated record set.

As in the proposed rule, in the final rule we provide that individuals have a right of access to protected health information that is maintained in a designated record set. This right applies to health plans, covered health care providers, and health care clearinghouses that create or receive protected health information other than as a business associate of another covered entity (see § 164.500(b)). In the final rule, however, we modify the definition of designated record set. For a discussion of the significant changes made to the definition of designated record set, see § 164.501 and the corresponding preamble.

Under the revised definition, individuals have a right of access to any protected health information that is used, in whole or in part, to make decisions about individuals. This information includes, for example, information used to make health care decisions or information used to determine whether an insurance claim will be paid. Covered entities often incorporate the same protected health information into a variety of different data systems, not all of which will be utilized to make decisions about individuals. For example, information systems that are used for quality control or peer review analyses may not be used to make decisions about individuals. In that case, the information systems would not fall within the definition of designated record set. We do not require entities to grant an individual access to protected health information maintained in these types of information systems.

Duration of the Right of Access

As in the proposed rule, covered entities must provide access to individuals for as long as the protected health information is maintained in a designated record set.

Exceptions to the Right of Access

In the NPRM, we proposed to establish a right for individuals to access any protected health information maintained in a designated record set. Though we proposed to permit covered entities to deny access in certain situations relating to the particular individual requesting access, we did not specifically exclude any protected health information from the right of access.

In the final rule, we specify three types of information to which individuals do not have a right of access, even if the information is maintained in a designated record set. They are psychotherapy notes, information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding, and certain protected health information maintained by a covered entity that is subject to or exempted from the Clinical Laboratory Improvements Amendments of 1988 (CLIA). Covered entities may, but are not required to, provide access to this information.

First, unlike the proposed rule, we specify that individuals do not have a right of access to psychotherapy notes.

Second, individuals do not have a right of access to information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding. In the NPRM, we would have permitted covered entities to deny a request for access to protected health information complied in reasonable anticipation of, or for use in, a legal proceeding. We change the language in the final rule to clarify that a legal proceeding includes civil, criminal, and administrative actions and proceedings. In the final rule, we clarify that an individual does not have a right to this information by including it in the list of exceptions rather than stating that a covered entity may deny access to this information. Under this exception, the covered entity may deny access to any information that relates specifically to legal preparations but may not deny access to the individual's underlying health information. We do not intend to require covered entities to provide access to documents protected by attorney work-product privilege nor do we intend to alter rules of discovery.

Third, unlike the proposed rule, individuals do not have a right of access to protected health information held by clinical laboratories if CLIA prohibits such access. CLIA states that clinical laboratories may provide clinical laboratory test records and reports only to ''authorized persons,'' as defined primarily by state law. The individual who is the subject of the information is not always included in this set of authorized persons. When an individual is not an authorized person, this restriction effectively prohibits the clinical laboratory from providing an individual access to this information. We do not intend to preempt CLIA and, therefore, do not require covered clinical laboratories to provide an individual access to this information if CLIA prohibits them from doing so. We note, however, that individuals have the right of access to this information if it is maintained by a covered health care provider, clearinghouse, or health plan that is not subject to CLIA.

Finally, unlike the proposed rule, individuals do not have access to protected health information held by certain research laboratories that are exempt from the CLIA regulations. The CLIA regulations specifically exempt the components or functions of ''research laboratories that test human specimens but do not report patient specific results for the diagnosis, prevention or treatment of any disease or impairment of, or the assessment of the health of individual patients.'' 42 CFR 493.3(a)(2). If subject to the access requirements, these laboratories, or the applicable components of them, would be forced to comply with the CLIA regulations once they provided an individual with the access under this privacy rule. Therefore, to alleviate this additional regulatory burden, we have exempted these laboratories, or the relevant components of them, from the access requirements of this regulation.

Grounds for Denial of Access

In the NPRM we proposed to permit covered health care providers and health plans to deny an individual access to inspect and copy protected health information about them for five reasons: (1) a licensed health care professional determined the inspection and copying was reasonably likely to endanger the life or physical safety of the individual or another person; (2) the information was about another person (other than a health care provider) and a licensed health care professional determined the inspection and copying was reasonably likely to cause substantial harm to that other person; (3) the information was obtained under a promise of confidentiality from someone other than a health care provider and the inspection and copying was likely to reveal the source of the information; (4) the information was obtained by a covered provider in the course of a clinical trial, the individual agreed to the denial of access in consenting to participate in the trial, and the trial was in progress; and (5) the information was compiled in reasonable anticipation of, or for use in, a legal

proceeding. In the NPRM, covered entities would not have been permitted to use these grounds to deny individuals access to protected health information that was also subject to the Privacy Act.

In the final rule, we retain all of these grounds for denial, with some modifications. One of the proposed grounds for denial (regarding legal proceedings) is retained as an exception to the right of access. (See discussion above.) We also include additional grounds for denial and create a right for individuals to request review of certain denials.

There are five types of denials covered entities may make without providing the individual with a right to have the denial reviewed.

First, a covered entity may deny an individual access to any information that is excepted from the right of access under § 164.524(a)(1). (See discussion above.)

Second, we add a new provision that permits a covered entity that is a correctional institution or covered health care provider acting under the direction of a correctional institution to deny an inmate's request to obtain a copy of protected health information if obtaining a copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or other inmates or the safety of any officer, employee or other person at the correctional institution or responsible for the transporting of the inmate. This ground for denial is restricted to an inmate's request to obtain a copy of protected health information. If an inmate requests inspection of protected health information, the request must be granted unless one of the other grounds for denial applies. The purpose for this exception, and the reason that the exception is limited to denying an inmate a copy and not to denying a right to inspect, is to give correctional institutions the ability to maintain order in these facilities and among inmates without denying an inmate the right to review his or her protected health information.

Third, as in the proposed rule, a covered entity may deny an individual access to protected health information obtained by a covered provider in the course of research that includes treatment of the research participants, while such research is in progress. For this exception to apply, the individual must have agreed to the denial of access in conjunction with the individual's consent to participate in the research and the covered provider must have informed the individual that the right of access will be reinstated upon completion of the research. If either of these conditions is not met, the individual has the right to inspect and copy the information (subject to the other exceptions we provide here). In all cases, the individual has the right to inspect and copy the information after the research is complete.

As with all the grounds for denial, covered entities are not required to deny access under the research exception. We expect all researchers to maintain a high level of ethical consideration for the welfare of research participants and provide access in appropriate circumstances. For example, if a participant has a severe adverse reaction, disclosure of information during the course of the research may be necessary to give the participant adequate information for proper treatment decisions.

Fourth, we clarify the ability of a covered entity to deny individuals access to protected health information that is also subject to the Privacy Act. In the final rule, we specify that a covered entity may deny an individual access to protected health information that is contained in records that are subject to the Privacy Act if such denial is permitted under the Privacy Act. This ground for denial exists in addition to the other grounds for denial available under this rule. If an individual requests access to protected health information that is also subject to the Privacy Act, a covered entity may deny access to that information for any of the reasons permitted under the Privacy Act and for any of the reasons permitted under this rule.

Fifth, as in the proposed rule, a covered entity may deny an individual access to protected health information if the covered entity obtained the requested information from someone other than a health care provider under a promise of confidentiality and such access would be reasonably likely to reveal the source of the information. This provision is intended to preserve a covered entity's ability to maintain an implicit or explicit promise of confidentiality. A covered entity may not, however, deny access to protected health information when the information has been obtained from a health care provider. An individual is entitled to have access to all information about him or her generated by the health care system (apart from the other exceptions we provide here). Confidentiality promises to health care providers should not interfere with that access.

As in the proposed rule, a covered entity may deny access to protected health information under certain circumstances in which the access may harm the individual or others. In the final rule, we specify that a covered entity may only deny access for these reasons if the covered entity provides the individual with a right to have the denial reviewed. (See below for a discussion of the right to review.)

There are three types of denials for which covered entities must provide the individual with a right to review. A denial under these provisions requires a determination by a licensed health care professional (such as a physician, physician's assistant, or nurse) based on an assessment of the particular circumstances and current professional medical standards of harm. Therefore, when the request is made to a health plan or clearinghouse, the covered entity will need to consult with a licensed health care professional before denying access under this provision.

First, as in the proposed rule, covered entities may deny individuals access to protected health information about them if a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person. The most commonly cited example is when an individual exhibits suicidal or homicidal tendencies. If a licensed health care professional determines that an individual exhibits such tendencies and that permitting inspection or copying of some of the individual's protected health information is reasonably likely to result in the individual committing suicide, murder, or other physical violence, then the health care professional may deny the individual access to that information. Under this reason for denial, covered entities may not deny access on the basis of the sensitivity of the health information or the potential for causing emotional or psychological harm.

Second, as in the proposed rule, covered entities may deny an individual access to protected health information if the information requested makes reference to someone other than the individual (and other than a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause serious harm to that other person. On some occasions when health information about one person is relevant to the care of another, a physician may incorporate it into the latter's record, such as information from group therapy sessions and information about illnesses with a genetic component. This provision permits a covered entity to withhold information in such cases if

the release of such information is reasonably likely to cause substantial physical, emotional, or psychological harm.

Third, we add a new provision regarding denial of access requested by personal representatives. Under § 164.502(g), a person that is a personal representative of an individual may exercise the rights of the individual, including the right to inspect and copy protected health information about the individual that is relevant to such person's representation. The provision permits covered entities to refuse to treat a personal representative as the individual, generally, if the covered entity has a reasonable belief that the individual has been or will be subjected to domestic violence, abuse or neglect by the personal representative, or that treating the personal representative as the individual may endanger the individual and, in its professional judgment, the covered entity decides that it is not in the best interest of the individual to treat such person as the personal representative.

In addition to that provision, we add a new provision at § 164.524(a)(3)(iii) to clarify that a covered entity may deny a request to inspect or copy protected health information if the information is requested by a personal representative of the individual and a licensed health care professional has determined that, in the exercise of professional judgment, such access is reasonably likely to cause substantial harm to the individual who is the subject of the information or to another person. The health care professional need not have a reasonable belief that the personal representative has abused or neglected the individuals and the harm that is likely to result need not be limited to the individual who is the subject of the requested protected health information. Therefore, a covered entity can recognize a person as a personal representative but deny such person access to protected health information as a personal representative.

We do not intend these provisions to create a legal duty for the covered entity to review all of the relevant protected health information before releasing it. Rather, we are preserving the flexibility and judgment of covered entities to deny access under appropriate circumstances. Denials are not mandatory; covered entities may always elect to provide requested health information to the individual. For each request by an individual, the covered entity may provide all of the information requested or evaluate the requested information, consider the circumstances surrounding the individual's request, and make a determination as to whether that request should be granted or denied, in whole or in part, in accordance with one of the reasons for denial under this rule. We intend to create narrow exceptions to the right of access and we expect covered entities to employ these exceptions rarely, if at all. Covered entities may only deny access for the reasons specifically provided in the rule.

Review of a Denial of Access

In the NPRM, we proposed to require covered entities, when denying an individual's request for access, to inform the individual of how to make a complaint to the covered entity and the Secretary.

We retain in the final rule the proposed approach (see below). In addition, if the covered entity denies the request on the basis of one of the reviewable grounds for denial described above, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny access. The covered entity must provide access in accordance with the reviewing official's determination. (See below for further description of the covered entity's requirements under § 164.524(d)(4) if the individual requests a review of denial of access.)

Section 164.524(b)—Requests for Access and Timely Action

In the NPRM, we proposed to require covered health care providers and health plans to provide a means for individuals to request access to protected health information about them. We proposed to require covered health care providers and health plans to take action on a request for access as soon as possible, but not later than 30 days following the request.

As in the proposed rule, the final rule requires covered entities to permit an individual to request access to inspect or to obtain a copy of the protected health information about the individual that is maintained in a designated record set. We additionally permit covered entities to require individuals to make requests for access in writing, if the individual is informed of this requirement.

In the final rule, we eliminate the requirement for the covered entity to act on a request as soon as possible. We recognize that circumstances may arise in which an individual will request access on an expedited basis. We encourage covered entities to have procedures in place for handling such requests. The time limitation is intended to be an outside deadline, rather than an expectation.

In the final rule, covered entities must act on a request for access within 30 days of receiving the request if the information is maintained or accessible on-site. Covered entities must act on a request for access within 60 days of receiving the request if the information is not maintained or accessible on-site. If the covered entity is unable to act on a request within the applicable deadline, it may extend the deadline by no more than 30 days by providing the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request. This written statement describing the extension must be provided within the standard deadline. A covered entity may only extend the deadline once per request for access. This provision permits a covered entity to take a total of up to 60 days to act on a request for access to information maintained on-site and up to 90 days to act on a request for access to information maintained off-site.

The requirements for a covered entity to comply with or deny a request for access, in whole or in part, are described below.

Section 164.524(c)—Provision of Access

In the NPRM, we proposed to require covered health care providers and health plans, upon accepting a request for access, to notify the individual of the decision and of any steps necessary to fulfill the request; to provide the information requested in the form or format requested, if readily producible in such form or format; and to facilitate the process of inspection and copying.

We generally retain the proposed approach in the final rule. If a covered entity accepts a request, in whole or in part, it must notify the individual of the decision and provide the access requested. Individuals have the right both to inspect and to copy protected health information in a designated record set. The individual may choose whether to inspect the information, to copy the information, or to do both.

In the final rule, we clarify that if the same protected health information is maintained in more than one designated record set or at more than one location, the covered entity is required to produce the information only once per request for access. We intend this provision to reduce covered entities' burden in complying with requests without reducing individuals' access to protected health information. We note that summary information and reports

are not the same as the underlying information on which the summary or report was based. Individuals have the right to obtain access both to summaries and to the underlying information. An individual retains the right of access to the underlying information even if the individual requests access to, or production of, a summary. (See below regarding requests for summaries.)

The covered entity must provide the information requested in the form or format requested if it is readily producible in such form or format. For example, if the covered entity maintains health information electronically and the individual requests an electronic copy, the covered entity must accommodate such request, if possible. Additionally, we specify that if the information is not available in the form or format requested, the covered entity must produce a readily readable hard copy of the information or another form or format to which the individual and covered entity can agree. If the individual agrees, including agreeing to any associated fees (see below), the covered entity may provide access to a summary of information rather than all protected health information in designated record sets. Similarly, a covered entity may provide an explanation in addition to the protected health information, if the individual agrees in advance to the explanation and any associated fees.

The covered entity must provide the access requested in a timely manner, as described above, and arrange for a mutually convenient time and place for the individual to inspect the protected health information or obtain a copy. If the individual requests that the covered entity mail a copy of the information, the covered entity must do so, and may charge certain fees for copying and mailing. For requests to inspect information that is maintained electronically, the covered entity may print a copy of the information and allow the individual to view the print-out on-site. Covered entities may discuss the request with the individual as necessary to facilitate the timely provision of access. For example, if the individual requested a copy of the information by mail, but the covered entity is able to provide the information faster by providing it electronically, the covered entity may discuss this option with the individual.

We proposed in the NPRM to permit the covered entity to charge a reasonable, cost-based fee for copying the information.

We clarify this provision in the final rule. If the individual requests a copy of protected health information, a covered entity may charge a reasonable, cost-based fee for the copying, including the labor and supply costs of copying. If hard copies are made, this would include the cost of paper. If electronic copies are made to a computer disk, this would include the cost of the computer disk. Covered entities may not charge any fees for retrieving or handling the information or for processing the request. If the individual requests the information to be mailed, the fee may include the cost of postage. Fees for copying and postage provided under state law, but not for other costs excluded under this rule, are presumed reasonable. If such per page costs include the cost of retrieving or handling the information, such costs are not acceptable under this rule.

If the individual requests an explanation or summary of the information provided, and agrees in advance to any associated fees, the covered entity may charge for preparing the explanation or summary as well.

The inclusion of a fee for copying is not intended to impede the ability of individuals to copy their records. Rather, it is intended to reduce the burden on covered entities. If the cost is excessively high, some individuals will not be able to obtain a copy. We encourage covered entities to limit the fee for copying so that it is within reach of all individuals.

We do not intend to affect the fees that covered entities charge for providing protected health information to anyone other than the individual. For example, we do not intend to affect current practices with respect to the fees one health care provider charges for forwarding records to another health care provider for treatment purposes.

Section 164.524(d)—Denial of Access

We proposed in the NPRM to require a covered health care provider or health plan that elects to deny a request for inspection or copying to make any other protected health information requested available to the individual to the extent possible, consistent with the denial.

In the final rule, we clarify the proposed approach. A covered entity that denies access, in whole or in part, must, to the extent possible, give the individual access to any other protected health information requested after excluding the protected health information to which the covered entity has a ground to deny access. We intend covered entities to redact or otherwise exclude only the information that falls within one or more of the denial criteria described above and to permit inspection and copying of all remaining information, to the extent it is possible to do so.

We also proposed to require covered providers and health plans, upon denying a request for access in whole or in part, to provide the individual with a written statement in plain language of the basis for the denial and how the individual could make a complaint to the covered entity or the Secretary.

We retain the proposed approach. A covered entity that denies access, in whole or in part, must provide the individual with a written denial in plain language that explains the basis for the denial. The written denial could include a direct reference to the section of the regulation relied upon for the denial, but the regulatory citation alone does not sufficiently explain the reason for the denial. The written denial must also describe how the individual can complain to the covered entity and the Secretary and must include the name or title and the telephone number of the covered entity's contact person or office that is responsible for receiving complaints.

In the final rule, we impose two additional requirements when the covered entity denies access, in whole or in part. First, if a covered entity denies a request on the basis of one of the reviewable grounds for denial, the written denial must describe the individual's right to a review of the denial and how the individual may exercise this right. Second, if the covered entity denies the request because it does not maintain the requested information, and the covered entity knows where the requested information is maintained, the covered entity must inform the individual where to direct the request for access.

Finally, we specify a covered entity's responsibilities when an individual requests a review of a denial. If the individual requests a review of a denial made under § 164.524(a)(3), the covered entity must designate a licensed health care professional to act as the reviewing official. This reviewing official must not have been involved in the original decision to deny access. The covered entity must promptly refer a request for review to the designated reviewing official. The reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards in § 164.524(a)(3). The covered entity must promptly provide the individual with written notice of the reviewing official's decision and otherwise carry out the decision in accordance with the requirements of this section.

Section 164.524(e)—Policies, Procedures, and Documentation

As in the proposed rule, we establish documentation requirements for covered entities that are subject to this provision. In accordance with § 164.530(j), the covered entity must retain documentation of the designated record sets that are subject to access by individuals and the titles of the persons or offices responsible for receiving and processing requests for access by individuals.

Section 164.526—Amendment of Protected Health Information

Section 164.526(a)—Right to Amend

In proposed § 164.516, we proposed to establish the individual's right to request a covered health care provider or health plan to amend or correct protected health information about the individual for as long as the covered entity maintains the information.

In § 164.526 of the final rule, we retain the general proposed approach, but establish an individual's right to have the covered entity amend, rather than amend or correct, protected health information. This right applies to protected health information and records in a designated record set for as long as the information is maintained in the designated record set. In the final rule, covered health care providers, health plans, and health care clearinghouses that create or receive protected health information other than as a business associate must comply with these requirements.

Denial of Amendment

We proposed to permit a covered health care provider or health plan to deny a request for amendment if it determined that the protected health information that was the subject of the request was not created by the covered provider or health plan, would not be available for inspection and copying under proposed § 164.514, or was accurate and complete. A covered entity would have been permitted, but not required, to deny a request if any of these conditions were met.

As in the proposed rule, the final rule permits a covered entity to deny a request for amendment if the covered entity did not create the protected health information or record that is the subject of the request for amendment. We add one exception to this provision: if the individual provides a reasonable basis to believe that the originator of the protected health information is no longer available to act on the requested amendment, the covered entity must address the request for amendment as though the covered entity had created the information.

As in the proposed rule, a covered entity also may deny a request for amendment if the protected health information that is the subject of the request for amendment is not part of a designated record set or would not otherwise be available for inspection under § 164.524. We eliminate the ability to deny a request for amendment if the information or record that is the subject of the request would not be available for copying under the rule. Under § 164.524(a)(2)(ii), an inmate may be denied a copy of protected health information about the inmate. We intend to preserve an inmate's ability to request amendments to information, even if a copy of the information would not be available to the inmate, subject to the other exceptions provided in this section.

Finally, as in the proposed rule, a covered entity may deny a request for amendment if the covered entity determines that the information in dispute is accurate and complete. We draw this concept from the Privacy Act of 1974, governing records held by federal agencies, which permits an individual to request correction or amendment of a record ''which the individual believes is not accurate, relevant, timely, or complete.'' (5 U.S.C. 552a(d)(2)). We adopt the standards of ''accuracy'' and ''completeness'' and draw on the clarification and analysis of these terms that have emerged in administrative and judicial interpretations of the Privacy Act during the last 25 years. We note that for federal agencies that are also covered entities, this rule does not diminish their present obligations under the Privacy Act of 1974.

This right is not intended to interfere with medical practice or to modify standard business record keeping practices. Perfect records are not required. Instead, a standard of reasonable accuracy and completeness should be used. In addition, this right is not intended to provide a procedure for substantive review of decisions such as coverage determinations by payors. It is intended only to affect the content of records, not the underlying truth or correctness of materials recounted therein. Attempts under the Privacy Act of 1974 to use this mechanism as a basis for collateral attack on agency determinations have generally been rejected by the courts. The same results are intended here.

Section 164.526(b)—Requests for Amendment and Timely Action

We proposed to require covered health care providers and health plans to provide a means for individuals to request amendment of protected health information about them. Under the NPRM, we would have required covered health care providers and health plans to take action on a request for amendment or correction within 60 days of the request.

As in the proposed rule, covered entities must permit individuals to request that the covered entity amend protected health information about them. We also permit certain specifications for the form and content of the request. If a covered entity informs individuals of such requirements in advance, a covered entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment. If the covered entity imposes such a requirement and informs individuals of the requirement in advance, the covered entity is not required to act on an individual's request that does not meet the requirements.

We retain the requirement for covered entities to act on a request for amendment within 60 days of receipt of the request. In the final rule, we specify the nature of the action the covered entity must take within the time frame. The covered entity must inform the individual, as described below, that the request has been either accepted or denied, in whole or in part. It must also take certain actions pursuant to its decision to accept or deny the request, as described below. If the covered entity is unable to meet the deadline, the covered entity may extend the deadline by no more than 30 days. The covered entity must inform the individual in writing, within the initial 60-day period, of the reason for the delay and the date by which the covered entity will complete its action on the request. A covered entity may only extend the deadline one time per request for amendment.

Section 164.526(c)—Accepting the Amendment

If a covered health care provider or health plan accepted a request for amendment, in whole or in part, we proposed to require the covered entity to make the appropriate change. The covered entity would have had to identify the challenged entries as amended or corrected and indicate the location of the amended or corrected information.

We also proposed to require the covered provider or health plan to make reasonable efforts to notify certain entities of the amendment: 1) entities the individual identified as needing to be notified and 2) entities the covered provider or health plan knew had received the erroneous or incomplete information and who may have relied, or could foreseeably rely, on such information to the detriment of the individual.

The covered provider or health plan would also have been required to notify the individual of the decision to amend the information.

As in the proposed rule, if a covered entity accepts an individual's request for amendment or correction, it must make the appropriate amendment. In the final rule, we clarify that, at a minimum, the covered entity must identify the records in the designated record set that are affected by the amendment and must append or otherwise provide a link to the location of the amendment. We do not require covered entities to expunge any protected health information. Covered entities may expunge information if doing so is consistent with other applicable law and the covered entity's record keeping practices.

We alter some of the required procedures for informing the individual and others of the accepted amendment. As in the proposed rule, the covered entity must inform individuals about accepted amendments. In the final rule, the covered entity must obtain the individual's agreement to have the amended information shared with certain persons. If the individual agrees, the covered entity must make reasonable efforts to provide a copy of the amendment within a reasonable time to: (1) Persons the individual identifies as having received protected health information about the individual and needing the amendment; and (2) persons, including business associates, that the covered entity knows have the unamended information and who may have relied, or could foreseeably rely, on the information to the detriment of the individual. For example, a covered entity must make reasonable efforts to inform a business associate that uses protected health information to make decisions about individuals about amendments to protected health information used for such decisions.

Section 164.526(d)—Denying the Amendment

If a covered health care provider or health plan denied a request for amendment, in whole or in part, we proposed to require the covered entity to provide the individual with a written statement in plain language of the basis for the denial, a description of how the individual could submit a written statement of disagreement with the denial, and a description of how the individual could make a complaint with the covered entity and the Secretary.

We proposed to require covered health care providers and health plans to have procedures to permit the individual to file a written statement of disagreement with the denial and to include the covered entity's statement of denial and the individual's statement of disagreement with any subsequent disclosure of the disputed information. Covered entities would have been permitted to establish a limit to the length of the individual's statement of disagreement and to summarize the statement if necessary. We also proposed to permit covered entities to provide a rebuttal to the individual's statement with future disclosures.

As in the proposed rule, if a covered entity denies a request for amendment, it must provide the individual with a statement of denial written in plain language. The written denial must include the basis for the denial, how the individual may file a written statement disagreeing with the denial, and how the individual may make a complaint to the covered entity and the Secretary.

In the final rule, we additionally require the covered entity to inform individuals of their options with respect to future disclosures of the disputed information in order to ensure that an individual is aware of his or her rights. The written denial must state that if the individual chooses not to file a statement of disagreement, the individual may request that the covered entity include the individual's request for amendment and the covered entity's denial of the request with any future disclosures of the protected health information that is the subject of the requested amendment.

As in the proposed rule, the covered entity must permit the individual to submit a written statement disagreeing with the denial and the basis of such disagreement. The covered entity may reasonably limit the length of a statement of disagreement and may prepare a written rebuttal to the individual's statement of disagreement. If the covered entity prepares a rebuttal, it must provide a copy to the individual.

The covered entity must identify the record or protected health information that is the subject of the disputed amendment and append or otherwise link the following information to the designated record set: the individual's request for amendment, the covered entity's denial of the request, the individual's statement of disagreement (if any), and the covered entity's rebuttal (if any). If the individual submits a written statement of disagreement, all of the appended or linked information, or an accurate summary of it, must be included with any subsequent disclosure of the protected health information to which the disagreement relates. If the individual does not submit a written statement of disagreement, the covered entity must include the appended or linked information only if the individual requests that the covered entity do so.

In the final rule, we clarify that when a subsequent disclosure is a standard transaction adopted under the Transactions Rule that cannot accommodate the additional materials described above, the covered entity may separately disclose the additional material to the recipient of the transaction.

Section 164.526(e)—Actions on Notices of Amendment

We proposed to require any covered entity that received a notification of amendment to have procedures in place to make the amendment in any of its designated record sets and to notify its business associates, if appropriate, of amendments.

We retain the proposed approach in the final rule. If a covered entity receives a notification of amended protected health information from another covered entity as described above, the covered entity must make the necessary amendment to protected health information in designated record sets it maintains. In addition, covered entities must require their business associates who receive such notifications to incorporate any necessary amendments to designated record sets maintained on the covered entity's behalf. (See § 164.504 regarding business associate requirements.)

Section 164.526(f)—Policies, 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), the covered entity must document the titles of the persons or offices responsible for receiving and processing requests for amendment.

§ 164.528—Accounting of Disclosures of Protected Health Information

Right to an Accounting of Disclosures

We proposed in the NPRM to grant individuals a right to receive an

accounting of all disclosures of protected health information about them by a covered entity for purposes other than treatment, payment, and health care operations. We proposed this right to exist for as long as the covered entity maintained the protected health information.

We also proposed that individuals would not have a right to an accounting of disclosures to health oversight or law enforcement agencies if the agency provided a written request for exclusion for a specified time period and the request stated that access by the individual during that time period would be reasonably likely to impede the agency's activities.

We generally retain the proposed approach in the final rule. As in the proposed rule, individuals have a right to receive an accounting of disclosures made by a covered entity, including disclosures by or to a business associate of the covered entity, for purposes other than treatment, payment, and health care operations, subject to certain exceptions as discussed below.

We revise the duration of this right under the final rule. Individuals have a right to an accounting of the applicable disclosures that have been made in the 6 year period prior to the date of a request for an accounting. We additionally clarify in § 164.528(b)(1) that an individual may request, and a covered entity may then provide, an accounting of disclosures for a period of time less than 6 years from the date of the request. For example, an individual could request an accounting only of disclosures that occurred during the year prior to the request.

In the final rule, we exclude several additional types of disclosures from the accounting requirement. Covered entities are not required to include in the accounting disclosures to the individual as provided in § 164.502; disclosures for facility directories, disclosures to persons involved in the individual's care, or other disclosures for notification purposes as provided in § 164.510; disclosures for national security or intelligence purposes as provided in § 164.512(k)(2); disclosures to correctional institutions or law enforcement officials as provided in § 164.512(k)(5); or any disclosures that were made by the covered entity prior to the compliance date of the rule for that covered entity.

We retain the time-limited exclusion for disclosures to health oversight and law enforcement agencies, but require rather than permit the exclusion for the specified time period. Covered entities must exclude disclosures to a health oversight agency or law enforcement official from the accounting for the time period specified by the applicable agency or official if the agency or official provides the covered entity with a statement that inclusion of the disclosure(s) in the accounting to the individual during that time period would be reasonably likely to impede the agency or official's activities. The agency or official's statement must specifically state how long the information must be excluded. At the expiration of that period, the covered entity is required to include the disclosure(s) in an accounting for the individual. If the agency or official's statement is made orally, the covered entity must document the identity of the agency or official who made the statement and must exclude the disclosure(s) for no longer than 30 days from the date of the oral statement, unless a written statement is provided during that time. If the agency or official provides a written statement, the covered entity must exclude the disclosure(s) for the time period specified in the written statement.

Content of the Accounting

We proposed in the NPRM to require the accounting to include all disclosures as described above, including disclosures authorized by the individual. The accounting would have been required to contain the date of each disclosure; the name and address of the organization or person who received the protected health information; a brief description of the information disclosed; and copies of all requests for disclosures. For disclosures other than those made at the request of the individual, the accounting would have also included the purpose for which the information was disclosed.

We generally retain the proposed approach in the final rule, but do not require covered entities to make copies of authorizations or other requests for disclosures available with the accounting. Instead, we require the accounting to contain a brief statement of the purpose of the disclosure. The statement must reasonably inform the individual of the basis for the disclosure. In lieu of the statement of purpose, a covered entity may include a copy of the individual's authorization under § 164.508 or a copy of a written request for disclosure, if any, under § 164.502(a)(2)(ii) or § 164.512. We also clarify that covered entities are only required to include the address of the recipient of the disclosed protected health information if the covered entity knows the address.

We add a provision allowing for a summary accounting of recurrent disclosures. For multiple disclosures to the same recipient pursuant to a single authorization under § 164.508 or for a single purpose under §§ 164.502(a)(2)(ii) or 164.512, the covered entity may provide a summary accounting addressing the series of disclosures rather than a detailed accounting of each disclosure in the series. In this circumstance, a covered entity may limit the accounting of the series of disclosures to the following information: the information otherwise required above for the first disclosure in the series during the accounting period; the frequency, periodicity, or number of disclosures made during the accounting period; and the date of the most recent disclosure in the series. For example, if under § 164.512(b), a covered entity discloses the same protected health information to a public health authority for the same purpose every month, it can account for those disclosures by including in the accounting the date of the first disclosure, the public health authority to whom the disclosures were made and the public health authority's address, a brief description of the information disclosed, a brief description of the purpose of the disclosures, the fact that the disclosures were made every month during the accounting period, and the date of the most recent disclosure.

Provision of the Accounting

We proposed in the NPRM to require covered entities to provide individuals with an accounting of disclosures as soon as possible, but not later than 30 days following receipt of the request for the accounting.

In the final rule, we eliminate the requirement for the covered entity to act as soon as possible. We recognize that circumstances may arise in which an individual will request an accounting on an expedited basis. We encourage covered entities to implement procedures for handling such requests. The time limitation is intended to be an outside deadline, rather than an expectation. We expect covered entities always to be attentive to the circumstances surrounding each request and to respond in an appropriate time frame.

In the final rule, covered entities must provide a requested accounting no later than 60 days after receipt of the request. If the covered entity is unable to meet the deadline, the covered entity may extend the deadline by no more than 30 days. The covered entity must inform the individual in writing, within the standard 60-day deadline, of the reason for the delay and the date by which the covered entity will provide the request.