marketing purposes, absent any other authority to act for her husband. See § 164.502(g) for more information regarding personal representatives.

Comment: One commenter suggested that authorizations should be dated on the day they are signed.

Response: We agree and have retained this requirement in the final rule.

Additional Elements and Requirements for Authorizations Requested by the Covered Entity for Its Own Uses and Disclosures

Comment: Some commenters suggested that we should not require different elements in authorizations initiated by the covered entity versus authorizations initiated by the individual. The commenters argued the standards were unnecessary, confusing, and burdensome.

Response: The proposed authorization requirements are intended to ensure that an individual's authorization is truly voluntary. The additional elements required for authorizations initiated by the covered entity for its own uses and disclosures or for receipt of protected health information from other covered entities to carry out treatment, payment, or health care operations address concerns that are unique to these forms of authorization. (See above regarding requirements for research authorizations under § 164.508(f).)

First, when applicable, these authorizations must state that the covered entity will not condition treatment, payment, eligibility, or enrollment on the individual's providing authorization for the requested use or disclosure. This statement is not appropriate for authorizations initiated by the individual or another person who does not have the ability to withhold services if the individual does not authorize the use or disclosure.

Second, the authorization must state that the individual may refuse to sign the authorization. This statement is intended to signal to the individual that the authorization is voluntary and may not be accurate if the authorization is obtained by a person other than a covered entity.

Third, these authorizations must describe the purpose of the use or disclosure. We do not include this element in the core requirements because we understand there may be times when the individual does not want the covered entity maintaining the protected health information to know the purpose for the use or disclosure. For example, an individual contemplating litigation may not want the covered entity to know that litigation is the purpose of the disclosure. If the covered entity is initiating the authorization for its own use or disclosure, however, the individual and the covered entity maintaining the protected health information should have a mutual understanding of the purpose of the use or disclosure. Similarly, when a covered entity is requesting authorization for a disclosure by another covered entity that may have already obtained the individual's consent for the disclosure, the individual and covered entity that maintains the protected health information should be aware of this potential conflict.

There are two additional requirements for authorizations requested by a covered entity for its own use or disclosure of protected health information it maintains. First, we require the covered entity to describe the individual's right to inspect or copy the protected health information to be used or disclosed. Individuals may want to review the information to be used or disclosed before signing the authorization and should be reminded of their ability to do so. This requirement is not appropriate for authorizations for a covered entity to receive protected health information from another covered entity, however, because the covered entity requesting the authorization is not the covered entity that maintains the protected health information and cannot, therefore, grant or describe the individual's right to access the information.

If applicable, we also require a covered entity that requests an authorization for its own use or disclosure to state that the use or disclosure of the protected health information will result in direct or indirect remuneration to the entity. Individuals should be aware of any conflicts of interest or financial incentives on the part of the covered entity requesting the use or disclosure. These statements are not appropriate, however, in relation to uses and disclosures to carry out treatment, payment, and health care operations. Uses and disclosures for these purposes will often involve remuneration by the nature of the use or disclosure, not due to any conflict of interest on the part of either covered entity.

We note that authorizations requested by a covered entity include authorizations requested by the covered entity's business associate on the covered entity's behalf. Authorizations requested by a business associate on the covered entity's behalf and that authorize the use or disclosure of protected health information by the covered entity or the business associate must meet the requirements in § 164.508(d). Similarly, authorizations requested by a business associate on behalf of a covered entity to accomplish the disclosure of protected health information to that business associate or covered entity as described in § 164.508(e) must meet the requirements of that provision.

We disagree that these elements are unnecessary, confusing, or burdensome. We require them to ensure that the individual has a complete understanding of what he or she is agreeing to permit.

Comment: Many commenters suggested we include in the regulation text a provision stated in the preamble that entities and their business partners must limit their uses and disclosures to the purpose(s) specified by the individual in the authorization.

Response: We agree. In accordance with § 164.508(a)(1), covered entities may only use or disclose protected health information consistent with the authorization. In accordance with § 164.504(e)(2), a business associate may not make any uses or disclosures that the covered entity couldn't make.

Comment: Some comments suggested that authorizations should identify the source and amount of financial gain, if any, resulting from the proposed disclosure. Others suggested that the proposed financial gain requirements were too burdensome and would decrease trust between patients and providers. Commenters recommended that the requirement either should be eliminated or should only require covered entities, when applicable, to state that direct and foreseeable financial gain to the covered entity will result. Others requested clarification of how the requirement for covered entities to disclose financial gain relates to the criminal penalties that accrue for offenses committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm. Some commenters advocated use of the term ''financial compensation'' rather than ''financial gain'' to avoid confusion with in-kind compensation rules. Some comments additionally suggested excluding marketing uses and disclosures from the requirements regarding financial gain.

Response: We agree that clarification is warranted. In § 164.508(d)(1)(iv) of the final rule, we require a covered entity that asks an individual to sign an authorization for the covered entity's use or disclosure of protected health information and that will receive direct

or indirect remuneration from a third party for the use or disclosure, to state that fact in the authorization. Remuneration from a third party includes payments such as a fixed price per disclosure, compensation for the costs of compiling and sending the information to be disclosed, and, with respect to marketing communications, a percentage of any sales generated by the marketing communication. For example, a device manufacturer may offer to pay a fixed price per name and address of individuals with a particular diagnosis, so that the device manufacturer can market its new device to people with the diagnosis. The device manufacturer may also offer the covered entity a percentage of the profits from any sales generated by the marketing materials sent. If a covered entity seeks an authorization to make such a disclosure, the authorization must state that the remuneration will occur. We believe individuals should have the opportunity to weigh the covered entity's potential conflict of interest when deciding to authorize the covered entity's use or disclosure of protected health information. We believe that the term ''remuneration from a third party'' clarifies our intent to describe a direct, tangible exchange, rather than the mere fact that parties intend to profit from their enterprises.

Comment: One commenter suggested we require covered entities to request authorizations in a manner that does not in itself disclose sensitive information.

Response: We agree that covered entities should make reasonable efforts to avoid unintentional disclosures. In § 164.530(c)(2), we require covered entities to have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

Comment: Some commenters requested clarification that covered entities are permitted to seek authorization at the time of enrollment or when individuals otherwise first interact with covered entities. Similarly, commenters requested clarification that covered entities may disclose protected health information created after the date the authorization was signed but prior to the expiration date of the authorization. These commenters were concerned that otherwise multiple authorizations would be required to accomplish a single purpose. Other comments suggested that we prohibit prospective authorizations (i.e., authorizations requested prior to the creation of the protected health information to be disclosed under the authorization) because it is not possible for individuals to make informed decisions about these authorizations.

Response: We confirm that covered entities may act on authorizations signed in advance of the creation of the protected health information to be released. We note, however, that all of the required elements must be completed, including a description of the protected health information to be used or disclosed pursuant to the authorization. This description must identify the information in a specific and meaningful fashion so that the individual can make an informed decision as to whether to sign the authorization.

Comment: Some commenters suggested that the final rule prohibit financial incentives, such as premium discounts, designed to encourage individuals to sign authorizations.

Response: We do not prohibit or require financial incentives for authorizations. We have attempted to ensure that authorizations are entered into voluntary. If a covered entity chooses to offer a financial incentive for the individual to sign the authorization, and the individual chooses to accept it, they are free to do so.

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

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

Comment: Many hospital organizations opposed the NPRM's proposed opt-in approach to disclosure of directory information. These groups noted the preamble's statement that most patients welcomed the convenience of having their name, location, and general condition included in the patient directory. They said that requiring hospitals to obtain authorization before including patient information in the directory would cause harm to many patients' needs in an effort to serve the needs of the small number of patients who may not want their information to be included. Specifically, they argued that the proposed approach ultimately could have the effect of making it difficult or impossible for clergy, family members, and florists to locate patients for legitimate purposes. In making this argument, commenters pointed to problems that occurred after enactment of privacy legislation in the State of Maine in 1999. The legislation, which never was officially implemented, was interpreted by hospitals to prohibit disclosure of patient information to directories without written consent. As a result, when hospitals began complying with the law based on their interpretation, family members and clergy had difficulty locating patients in the hospital.

Response: We share commenters' concern about the need to ensure that family members and clergy who have a legitimate need to locate patients are not prevented from doing so by excessively stringent restrictions on disclosure of protected health information to health care facilities' directories. Accordingly, the final rule takes an opt-out approach, stating that health care institutions may include the name, general condition, religious affiliation, and location of a patient within the facility in the facility's directory unless the patient explicitly objects to the use or disclosure of protected health information for directory purposes. To ensure that this opt-out can be exercised, the final rule requires facilities to notify individuals of their right not to be included in the directory and to give them the opportunity to opt out. The final rule indicates that the notice and opt-out may be oral. The final rule that allows health care facilities to disclose to clergy the four types of protected health information specified above without requiring the clergy to ask for the individual by name will allow the clergy to identify the members of his or her faith who are in the facility, thus ensuring that this rule will not significantly interfere with the exercise of religion, including the clergy's traditional religious mission to provide services to individuals.

Comment: A small number of commenters recommended requiring written authorization for all disclosures of protected health information for directory purposes. These commenters believed that the NPRM's proposed provision allowing oral agreement would not provide sufficient privacy protection; that it did not sufficiently hold providers accountable for complying with patient wishes; and that it could create liability issues for providers.

Response: The final rule does not require written authorization for disclosure of protected health information for directory purposes. We believe that requiring written authorization in these cases would increase substantially the administrative burdens and costs for covered health care providers and could lead to significant inconvenience for families and others attempting to locate individuals in health care institutions. Experience from the State of Maine suggests that requiring written authorization before patient information may be included in facility directories

can be disruptive for providers, families, clergy, and others.

Comment: Domestic violence organizations raised concerns that including information about domestic violence victims in health care facilities' directories could result in further harm to victims. The NPRM addressed the issue of potential danger to patients by stating that when patients were incapacitated, covered health care providers could exercise discretion—consistent with good medical practice and prior expression of patient preference—regarding whether to disclose protected health information for directory purposes. Several commenters recommended prohibiting providers from including information in a health care facility's directory about incapacitated individuals when the provider reasonably believed that the injuries to the individual could have been caused by domestic violence. These groups believed that such a prohibition was necessary to prevent abusers from locating and causing further harm to domestic violence patients.

Response: We share commenters' concerns about protecting victims of domestic violence from further abuse. We are also concerned, however, that imposing an affirmative duty on institutions not to disclose information any time injuries to the individual could have been the result of domestic violence would place too high a burden on health care facilities, essentially requiring them to rule out domestic violence as a potential cause of the injuries before disclosing to family members that an incapacitated person is in the institution.

We do believe, however, that it is appropriate to require covered health care providers to consider whether including the individual's name and location in the directory could lead to serious harm. As in the preamble to the NPRM, in the preamble to the final rule, we encourage covered health care providers to consider several factors when deciding whether to include an incapacitated patient's information in a health care facility's directory. One of these factors is whether disclosing an individual's presence in the facility could reasonably cause harm or danger to the individual (for example, if it appeared that an unconscious patient had been abused and disclosing that the individual is in the facility could give the attacker sufficient information to seek out the person and repeat the abuse). Under the final rule, when the opportunity to object to uses and disclosures for a facility's directory cannot practicably be provided due to an individual's incapacity or an emergency treatment circumstance, covered health care providers may use or disclose some or all of the protected health information that the rule allows to be included in the directory, if the disclosure is: (1) consistent with the individual's prior expressed preference, if known to the covered health care provider; and (2) in the individual's best interest, as determined by the covered health care provider in the exercise of professional judgement. The rule allows covered health care providers making decisions about incapacitated patients to include some portions of the patient's information (such as name) but not other information (such as location in the facility) to protect patient interests.

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

Comment: A number of comments supported the NPRM's proposed approach, which would have allowed covered entities to disclose protected health information to the individual's next of kin, family members, or other close personal friends when the individual verbally agreed to the disclosure. These commenters agreed that the presumption should favor disclosures to the next of kin, and they believed that health care providers should encourage individuals to share genetic information and information about transmittable diseases with family members at risk. Others agreed with the general approach but suggested the individual's agreement be noted in the medical record. These commenters also supported the NPRM's proposed reliance on good professional practices and ethics to determine when disclosures should be made to the next of kin when the individual's agreement could not practicably be obtained.

A few commenters recommended that the individual's agreement be in writing for the protection of the covered entity and to facilitate the monitoring of compliance with the individual's wishes. These commenters were concerned that, absent the individual's written agreement, the covered entity would become embroiled in intra-family disputes concerning the disclosures. Others argued that the individual's authorization should be obtained for all disclosures, even to the next of kin.

One commenter favored disclosures to family members and others unless the individual actively objected, as long as the disclosure was consistent with sound professional practice. Others believed that no agreement by the individual was necessary unless sensitive medical information would be disclosed or unless the health care provider was aware of the individual's prior objection. These commenters recommended that good professional practice and ethics determine when disclosures were appropriate and that disclosure should relate only to the individual's current treatment. A health care provider organization said that the ethical and legal obligations of the medical professional alone should control in this area, although it believed the proposed rule was generally consistent with these obligations.

Response: The diversity of comments regarding the proposal on disclosures to family members, next of kin, and other persons, reflects a wide range of current practice and individual expectations. We believe that the NPRM struck the proper balance between the competing interests of individual privacy and the need that covered health care providers may have, in some cases, to have routine, informal conversations with an individual's family and friends regarding the individual's treatment.

We do not agree with the comments stating that all such disclosures should be made only with consent or with the individual's written authorization. The rule does not prohibit obtaining the agreement of the individual in writing; however, we believe that imposing a requirement for consent or written authorization in all cases for disclosures to individuals involved in a person's care would be unduly burdensome for all parties. In the final rule, we clarify the circumstances in which such disclosures are permissible. The rule allows covered entities to disclose to family members, other relatives, close personal friends of the individual, or any other person identified by the individual, the protected health information directly relevant to such person's involvement with the individual's care or payment related to the individual's health care. In addition, the final rule allows covered entities to use or disclose protected health information to notify, or assist in the notification of (including identifying or locating) a family member, a personal representative of the individual, or another person responsible for the care of the individual, of the individual's location, general condition, or death. 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 can 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 the individual's care; (2) provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or (3) reasonably infers from the circumstances, based on the exercise of professional judgement, that the individual does not object to the disclosure. The final rule continues to permit disclosures in circumstances when the individual is not present 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. In such instances, covered entities may, in the exercise of professional judgement, 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.

As discussed in the preamble for this section, we do not intend to disrupt most covered entities' current practices with respect to informing family members and others with whom a patient has a close personal relationship about a patient's specific health condition when a patient is incapacitated due to a medical emergency and the family member or close personal friend comes to the covered entity to ask about the patient's condition. To the extent that disclosures to family members and others in these situations currently are allowed under state law and covered entities' own rules, § 164.510(b) allows covered entities to continue making them in these situations, consistent with the exercise of professional judgement as to the patient's best interest. As indicated in the preamble above, 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.

Comments: A few comments supported the NPRM approach because it permitted the current practice of allowing someone other than the patient to pick up prescriptions at pharmacies. One commenter noted that this practice occurs with respect to 25–40% of the prescriptions dispensed by community retail pharmacies. These commenters strongly supported the proposal's reliance on the professional judgement of pharmacists in allowing others to pick up prescriptions for bedridden or otherwise incapacitated patients, noting that in most cases it would be impracticable to verify that the person was acting with the individual's permission. Two commenters requested that the rule specifically allow this practice. One comment opposed the practice of giving prescriptions to another person without the individual's authorization, because a prescription implicitly could disclose medical information about the individual.

Response: As stated in the NPRM, we intended for this provision to authorize pharmacies to dispense prescriptions to family or friends who are sent by the individual to the pharmacy to pick up the prescription. We believe that stringent consent or verification requirements would place an unreasonable burden on numerous transactions. In addition, such requirements would be contrary to the expectations and preferences of all parties to these transactions. Although prescriptions are protected health information under the rule, we believe that the risk to individual privacy in allowing this practice to continue is minimal. We agree with the suggestion that the final rule should state explicitly that pharmacies have the authority to operate in this manner. Therefore, we have added a sentence to § 164.510(b)(3) allowing covered entities to use professional judgement and experience with common practice to make reasonable inferences of an individual's best interest in allowing a person to act on the individual's behalf to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information. In such situations, as when making disclosures of protected health information about an individual who is not present or is unable to agree to such disclosures, covered entities should disclose only information which directly relates to the person's involvement in the individual's current health care. Thus, when dispensing a prescription to a friend who is picking it up on the patient's behalf, the pharmacist should not disclose unrelated health information about medications that the patient has taken in the past which could prove embarrassing to the patient.

Comment: We received a few comments that misunderstood the provision as addressing disclosures related to deceased individuals.

Response: We understand that use of the term next of kin in this section may cause confusion. To promote clarity in the final rule, we eliminate the term ''next of kin,'' as well as the term's proposed definition. In the final rule, we address comments on next of kin and the deceased in the section on disclosure of protected health information about deceased individuals in § 164.512(g).

Comments: A number of commenters expressed concern for the interaction of the proposed section with state laws. Some of these comments interpreted the NPRM's use of the term next of kin as referring to individuals with health care power of attorney and thus they believed that the proposed rule's approach to next of kin was inappropriately informal and in conflict with state law. Others noted that some state laws did not allow health care information to be disclosed to family or friends without consent or other authorization. One commenter said that case law may be evolving toward imposing a more affirmative duty on health care practitioners to inform next of kin in a variety of circumstances. One commenter noted that state laws may not define clearly who is considered to be the next of kin.

Response: The intent of this provision was not to interfere with or change current practice regarding health care powers of attorney or the designation of other personal representatives. Such designations are formal, legal actions which give others the ability to exercise the rights of or make treatment decisions related to individuals. While persons with health care powers of attorney could have access to protected health information under the personal representatives provision (§ 164.502(g)), and covered entities may disclose to such persons under this provision, such disclosures do not give these individuals substantive authority to act for or on behalf of the individual with respect to health care decisions. State law requirements regarding health care powers of attorney continue to apply.

The comments suggesting that state laws may not allow the disclosures otherwise permitted by this provision or, conversely, that they may impose a more affirmative duty, did not provide any specifics with which to judge the affect of such laws. In general, however, state laws that are more protective of an individual's privacy interests than the rule by prohibiting a disclosure of protected health information continue to apply. The rule's provisions regarding disclosure of protected health information to family or friends of the individual are permissive only, enabling covered entities to abide by more stringent state laws without violating our rules. Furthermore, if the state law creates an affirmative and binding legal obligation on the covered entity to make disclosures to family or other persons under specific circumstances, the final rule allows covered entities to comply

with these legal obligations. See § 164.512(a).

Comments: A number of commenters supported the proposal to limit disclosures to family or friends to the protected health information that is directly relevant to that person's involvement in the individual's health care. Some comments suggested that this standard apply to all disclosures to family or friends, even when the individual has agreed to or not objected to the disclosure. One commenter objected to the proposal, stating that it would be too difficult to administer. According to this comment, it is accepted practice for health care providers to communicate with family and friends about an individual's condition, regardless of whether the person is responsible for or otherwise involved in the individual's care.

Other comments expressed concern for disclosures related to particular types of information. For example, two commenters recommended that psychotherapy notes not be disclosed without patient authorization. One commenter suggested that certain sensitive medical information associated with social stigma not be disclosed to family members or others without patient consent.

Response: We agree with commenters who advocated limiting permissible disclosures to relatives and close personal friends to information consistent with a person's involvement in the individual's care. Under the final rule, we clarify the NPRM provision to state that covered entities may disclose protected health information to family members, relatives, or close personal friends of an individual or any other person identified by the individual, to the extent that the information directly relates to the person's involvement in the individual's current health care. It is not intended to allow disclosure of past medical history that is not relevant to the individual's current condition. In addition, as discussed above, we do not intend to disrupt covered entities' current practices with respect to disclosing specific information about a patient's condition to family members or others when the individual is incapacitated due to a medical emergency and the family member or other individual comes to the covered entity seeking specific information about the patient's condition. For example, this section allows a hospital to disclose to a family member the fact that a patient had a heart attack, and to provide updated information to the family member about the patient's progress and prognosis during his or her period of incapacity.

We agree with the recommendation to require written authorization for a disclosure of psychotherapy notes to family, close personal friends, or others involved in the individual's care. As discussed below, the final rule allows disclosure of psychotherapy notes without authorization in a few limited circumstances; disclosure to individuals involved in a person's care is not among those circumstances. See § 164.508 for a further discussion of the final rule's provisions regarding disclosure of psychotherapy notes.

We do not agree, however, with the suggestion to treat some medical information as more sensitive than others. In most cases, individuals will have the opportunity to prohibit or limit such disclosures. For situations in which an individual is unable to do so, covered entities may, in the exercise of professional judgement, 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.

Comment: One commenter suggested that this provision should allow disclosure of protected health information to the clergy and to the Red Cross. The commenter noted that clergy have ethical obligations to ensure confidentiality and that the Red Cross often notifies the next of kin regarding an individual's condition in certain circumstances. Another commenter recommended allowing disclosures to law enforcement for the purpose of contacting the next of kin of individuals who have been injured or killed. One commenter sought clarification that ''close personal friend'' was intended to include domestic partners and same-sex couples in committed relationships.

Response: As discussed above, § 164.510(a) allows covered health care providers to disclose to clergy protected health information from a health care facility's directory. Under § 164.510(b), an individual may identify any person, including clergy, as involved in his or her care. This approach provides more flexibility than the proposed rule would have provided.

As discussed in the preamble of the final rule, this provision allows disclosures to domestic partners and others in same-sex relationships when such individuals are involved in an individual's care or are the point of contact for notification in a disaster. We do not intend to change current practices with respect to involvement of others in an individual's treatment decisions; informal information-sharing among persons involved; or the sharing of protected health information during a disaster. As noted above, a power of attorney or other legal relationship to an individual is not necessary for these informal discussions about the individual for the purpose of assisting in or providing a service related to the individual's care.

We agree with the comments noting that the Red Cross and other organizations may play an important role in locating and communicating with the family about individuals injured or killed in an accident or disaster situation. Therefore, the final rule includes new language, in § 164.510(b)(4), which allows covered entities to use or disclose protected health information to a public or private entity authorized by law or its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities to notify, or assist in the notification of (including identifying or locating) a family member, an individual's personal representative, or another person responsible for the individual's care regarding the individual's location, general condition, or death. The Red Cross is an example of a private entity that may obtain protected health information pursuant to these provisions. We recognize the role of the Red Cross and similar organizations in disaster relief efforts, and we encourage cooperation with these entities in notification efforts and other means of assistance.

Comment: One commenter recommended stating that individuals who are mentally retarded and unable to agree to disclosures under this provision do not, thereby, lose their access to further medical treatment. This commenter also proposed stating that mentally retarded individuals who are able to provide agreement have the right to control the disclosure of their protected health information. The commenter expressed concern that the parent, relative, or other person acting *in loco parentis* may not have the individual's best interest in mind in seeking or authorizing for the individual the disclosure of protected health information.

Response: The final rule regulates only uses and disclosures of protected health information, not the delivery of health care. Under the final rule's section on personal representatives (§ 164.502(g)), a person with authority to make decisions about the health care of an individual, under applicable law, may make decisions about the protected health information of that individual, to the extent that the protected health information is relevant to such person's representation.

In the final rule, § 164.510(b) may apply to permit disclosures to a person other than a personal representative. Under § 164.510(b), when an 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 protected health information to the third parties involved in the individual's 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. These conditions apply to disclosure of protected health information about individuals with mental retardation as well as to disclosures about all other individuals. Thus we do not believe it is necessary to include in this section of the final rule any language specifically on persons with mental retardation.

Comments: A few commenters recommended that disclosures made in good faith to the family or friends of the individual not be subject to sanctions by the Secretary, even if the covered entity had not fully complied with the requirements of this provision. One commenter believed that a fear of sanction would make covered entities overly cautious, such that they would not disclose protected health information to domestic partners or others not recognized by law as next of kin. Another commenter recommended that sanctions not be imposed if the covered entity has proper policies in place and has trained its staff appropriately. According to this commenter, the lack of documentation of disclosures in a particular case or medical record should not subject the entity to sanctions if the information was disclosed in good faith.

Response: We generally agree with commenters regarding disclosure in good faith pursuant to this provision. As discussed above, the final rule expands the scope of individuals to whom covered entities may disclose protected health information pursuant to this section. In addition, we delete the term next of kin, to avoid the appearance of requiring any legal determination of a person's relationship in situations involving informal disclosures. Similarly, consistent with the informal nature of disclosures pursuant to this section, we do not require covered entities to document such disclosures. If a covered entity imposes its own documentation requirements and a particular covered health care provider does not follow the entity's documentation requirements, the disclosure is not a violation of this rule.

Comments: The majority of comments on this provision were from individuals and organizations concerned about domestic violence. Most of these commenters wanted assurance that domestic violence would be a consideration in any disclosure to the spouse or relatives of an individual whom the covered entity suspected to be a victim of domestic violence or abuse. In particular, these commenters recommended that disclosures not be made to family members suspected of being the abuser if to do so would further endanger the individual. Commenters believed that this limitation was particularly important when the individual was unconscious or otherwise unable to object to the disclosures.

Response: We agree with the comments that victims of domestic violence and other forms of abuse need special consideration in order to avoid further harm, and we provide for discretion of a covered entity to determine that protected health information not be disclosed pursuant to § 164.510(b). Section 164.510(b) of the final rule, disclosures to family or friends involved in the individual's care, states that when an individual is unable to agree or object to the disclosure due to incapacity or another emergency situation, a covered entity must determine based on the exercise of professional judgment whether it is in the individual's best interest to disclose the information. As stated in the preamble, we intend for this exercise of professional judgment in the individual's best interest to account for the potential for harm to the individual in cases involving domestic violence. These circumstances are unique and are best decided by a covered entity, in the exercise of professional judgment, in each situation rather than by a blanket rule.

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

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

Comment: Numerous commenters addressed directly or by implication the question of whether the provision permitting uses and disclosures of protected health information if required by other law was necessary. Other commenters generally endorsed the need for such a provision. One such commenter approved of the provision as a needed fail-safe mechanism should the enumeration of permissible uses and disclosures of protected health information in the NPRM prove to be incomplete. Other commenters cited specific statutes which required access to protected health information, arguing that such a provision was necessary to ensure that these legally mandated disclosures would continue to be permitted. For example, some commenters argued for continued access to protected health information to investigate and remedy abuse and neglect as currently required by the Developmental Disabilities Assistance and Bill of Rights, 42 U.S.C. 6042, and the Protection and Advocacy for Mentally Ill Individuals Act, 42 U.S.C. 10801.

Some comments urged deletion of the provision for uses and disclosures required by other law. This concern appeared to be based on a generalized concern that the provision fostered government intrusion into individual medical information.

Finally, a number of commenters also urged that the required by law provision be deleted. These commenters argued that the proposed provision would have undermined the intent of the statute to preempt state laws which were less protective of individual privacy. As stated in these comments, the provision for uses and disclosures required by other law was ''broadly written and could apply to a variety of state laws that are contrary to the proposed rule and less protective of privacy. (Indeed, a law *requiring* disclosure is the least protective of privacy since it allows for no discretion.) The breadth of this provision greatly exceeds the exceptions to preemption contained in HIPAA.''

Response: We agree with the comments that proposed § 164.510(n) was necessary to harmonize the rule with existing state and federal laws mandating uses and disclosures of protected health information. Therefore, in the final rule, the provision permitting uses and disclosures as required by other law is retained. To accommodate other reorganization of the final rule, this provision has been designated as § 164.512(a).

We do not agree with the comments expressing concern for increased governmental intrusion into individual privacy under this provision. The final rule does not create any new duty or obligation to disclose protected health information. Rather, it permits covered entities to use or disclose protected health information when they are required by law to do so.

We likewise disagree with the characterization of the proposed provision as inconsistent with or contrary to the preemption standards in the statute or Part 160 of the rule. As described in the NPRM, we intend this provision to preserve access to information considered important enough by state or federal authorities to require its disclosure by law.

The importance of these required uses or disclosures is evidenced by the legislative or other public process necessary for the government to create a legally binding obligation on a covered entity. Furthermore, such required uses and disclosures arise in a myriad of other areas of law, ranging from topics addressing national security (uses and disclosures to obtain security clearances), to public health (reporting of communicable diseases), to law enforcement (disclosures of gun shot wounds). Required uses and disclosures also may address broad national concerns or particular regional or state concerns. It is not possible, or appropriate, for HHS to reassess the legitimacy of or the need for each of these mandates in each of their specialized contexts. In some cases where particular concerns have been raised by legal mandates in other laws, we allow disclosure as required by law, and we establish additional requirements to protect privacy (for example, informing the individual as required in § 164.512(c)) when covered entities make a legally mandated disclosure.

We also disagree with commenters who suggest that the approach in the final rule is contrary to the preemption provisions in HIPAA. HIPAA provides HHS with broad discretion in fashioning privacy protections. Recognizing the legitimacy of existing legal requirements is certainly within the Secretary's discretion. Additionally, given the variety of these laws, the varied contexts in which they arise, and their significance in ensuring that important public policies are achieved, we do not believe that Congress intended to preempt each such law unless HHS specifically recognized the law or purpose in the regulation.

Comment: A number of commenters urged that the provision permitting uses and disclosures required by other law be amended by deleting the last sentence which stated: ''This paragraph does not apply to uses or disclosures that are covered by paragraphs (b) through (m) of this section.'' Some commenters sought deletion of this sentence to avoid any inadvertent preemption of mandatory reporting laws, and requested clarification of the effect on specific statutes.

The majority of the commenters focused their concerns on the potential conflict between mandatory reporting laws to law enforcement and the limitations imposed by proposed § 164.510(f), on uses and disclosures to law enforcement. For example, the comments raised concerns that mandatory reporting to law enforcement of injuries resulting from violent acts and abuse require the health care provider to initiate such reports to local law enforcement or other state agencies, while the NPRM would have allowed such reporting on victims of crimes only in response to specific law enforcement requests for information. Similarly, mandatory reports of violence-related injuries may implicate suspected perpetrators, as well as victims, and compliance with such laws could be blocked by the proposed requirement that disclosures about suspects was similarly limited to a response to law enforcement inquiries for the specific purpose of identifying the suspect. The NPRM also would have limited the type of protected health information that could have been disclosed about a suspect or fugitive.

In general, commenters sought to resolve this overlap by removing the condition that the required-by-other-law provision applied only when no other national priority purpose addressed the particular use or disclosure. The suggested change would permit the covered entity to comply with legally mandated uses and disclosures as long as the relevant requirements of that law were met. Alternatively, other commenters suggested that the restrictions on disclosures to law enforcement be lifted to permit full compliance with laws requiring reporting for these purposes.

Finally, some comments sought clarification of when a use or disclosure was ''covered by paragraphs (b) through (m).'' These commenters were confused as to whether a particular use or disclosure had to be specifically addressed by another provision of the rule or simply within the scope of the one of the national priority purposes specified by proposed paragraphs (b) through (m).

Response: We agree with the commenters that the provision as proposed would have inadvertently interfered with many state and federal laws mandating the reporting to law enforcement or others of protected health information.

In response to these comments, we have modified the final rule to clarify how this section interacts with the other provisions in the rule.

Comment: A number of commenters sought expanded authority to use and disclosure protected health information when permitted by other law, not just when required by law. These comments specified a number of significant duties or potential societal benefits from disclosures currently permitted or authorized by law, and they expressed concern should these beneficial uses and disclosures no longer be allowed if not specifically recognized by the rule. For example, one commenter listed 25 disclosures of health records that are currently permitted, but not required, by state law. This commenter was concerned that many of these authorized uses and disclosures would not be covered by any of the national priority purposes specified in the NPRM, and, therefore, would not be a permissible use or disclosure under the rule. To preserve these important uses and disclosures, the comments recommended that provision be made for any use or disclosure which is authorized or permitted by other law.

Response: We do not agree with the comments that seek general authority to use and disclose protected health information as permitted, but not required, by other law. The uses and disclosures permitted in the final rule reflect those purposes and circumstances which we believe are of sufficient national importance or relevance to the needs of the health care system to warrant the use or disclosure of protected health information in the absence of either the individual's express authorization or a legal duty to make such use or disclosure. In permitting specific uses and disclosures that are not required by law, we have considered the individual privacy interests at stake in each area and crafted conditions or limitations in each identified area as appropriate to balance the competing public purposes and individual privacy needs. A general rule authorizing any use or disclosure that is permitted, but not required, by other law would undermine the careful balancing in the final rule.

In making this judgment, we have distinguished between laws that mandate uses or disclosures and laws that merely permit them. In the former case, jurisdictions have determined that public policy purposes cannot be achieved absent the use of certain protected health information, and we have chosen in general not to disturb their judgments. On the other hand, where jurisdictions have determined that certain protected health information is not necessary to achieve

a public policy purpose, and only have permitted its use or disclosure, we do not believe that those judgments reflect an interest in use or disclosure strong enough to override the Congressional goal of protecting privacy rights.

Moreover, the comments failed to present any compelling circumstance to warrant such a general provision. Despite commenters' concerns to the contrary, most of the beneficial uses and disclosures that the commenters referenced to support a general provision were, in fact, uses or disclosures already permissible under the rule. For example, the general statutory authorities relied on by one state health agency to investigate disease outbreaks or to comply with health data-gathering guidelines for reporting to certain federal agencies are permissible disclosures to public health agencies.

Finally, in the final rule, we add new provisions to § 164.512 to address three examples raised by commenters of uses and disclosures that are authorized or permitted by law, but may not be required by law. First, commenters expressed concern for the states that provide for voluntary reporting to law enforcement or state protective services of domestic violence or of abuse, neglect or exploitation of the elderly or other vulnerable adults. As discussed below, a new section, § 164.512(c), has been added to the final rule to specifically address uses and disclosures of protected health information in cases of abuse, neglect, or domestic violence. Second, commenters were concerned about state or federal laws that permitted coordination and cooperation with organizations or entities involved in cadaveric organ, eye, or tissue donation and transplantation. In the final rule, we add a new section, § 164.512(h), to permit disclosures to facilitate such donation and transplantation functions. Third, a number of commenters expressed concern for uses and disclosure permitted by law in certain custodial settings, such as those involving correctional or detention facilities. In the final rule, we add a new subsection to the section on uses and disclosures for specialized government functions, § 164.512(k), to identify custodial settings in which special rules are necessary and to specify the additional uses and disclosures of the protected health information of inmates or detainees which are necessary in such facilities.

Comment: A number of commenters asked for clarification of the term ''law'' and the phrase ''required by law'' for purposes of the provision permitting uses or disclosures that are required by law. Some of the commenters noted that ''state law'' was a defined term in Part 160 of the NPRM and that the terms should be used consistently. Other commenters were concerned about differentiating between laws that required a use or disclosure and those that merely authorize or permit a use or disclosure. A number of commenters recommended that the final rule include a definitive list of the laws that mandate a use or disclosure of protected health information.

Response: In the final rule, we clarify that, consistent with the ''state law'' definition in § 160.202, ''law'' is intended to be read broadly to include the full array of binding legal authority, such as constitutions, statutes, rules, regulations, common law, or other governmental actions having the effect of law. However, for the purposes of § 164.512(a), law is not limited to state action; rather, it encompasses federal, state or local actions with legally binding effect, as well as those by territorial and tribal governments.

For more detail on the meaning of ''required by law,'' see § 164.501. Only where the law imposes a duty on the health care professional to report would the disclosure be considered to be required by law.

The final rule does not include a definitive list of the laws that contain legal mandates for disclosures of protected health information. In light of the breadth of the term ''law'' and number of federal, state, local, and territorial or tribal authorities that may engage in the promulgation of binding legal authority, it would be impossible to compile and maintain such a list. Covered entities have an independent duty to be aware of their legal obligations to federal, state, local and territorial or tribal authorities. The rule's approach is simply intended to avoid any obstruction to the health plan or covered health care provider's ability to comply with its existing legal obligations.

Comment: A number of commenters recommended that the rule compel covered entities to use or disclose protected health information as required by law. They expressed concern that covered entities could refuse or delay compliance with legally mandated disclosures by misplaced reliance on a rule that permits, but does not require, a use or disclosure required by other law.

Response: We do not agree that the final rule should require covered entities to comply with uses or disclosures of protected health information mandated by law. The purpose of this rule is to protect privacy, and to allow those disclosures consistent with sound public policy. Consistent with this purpose, we mandate disclosure only to the individual who is the subject of the information, and for purposes of enforcing the rule. Where a law imposes a legal duty on the covered entity to use or disclose protected health information, it is sufficient that the privacy rule permit the covered entity to comply with such law. The enforcement of that legal duty, however, is a matter for that other law.

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

Comment: Several non-profit entities commented that medical records research by nonprofit entities to ensure public health goals, such as disease-specific registries, would not have been covered by this provision. These organizations collect information without relying on a government agency or law. Commenters asserted that such activities are essential and must continue. They generally supported the provisions allowing the collection of individually identifiable health information without authorization for registries. One stated that both governmental and non-governmental cancer registries should be exempt from the regulation. They stated that ''such entities, by their very nature, collect health information for legitimate public health and research purposes.'' Another, however, addressed its comments only to ''disclosure to non-government entities operating such system as required or authorized by law.''

Response: We acknowledge that such entities may be engaged in disease-specific or other data collection activities that provide a benefit to their members and others affected by a particular malady and that they contribute to the public health and scientific database on low incidence or little known conditions. However, in the absence of some nexus to a government public health authority or other underlying legal authority, it is unclear upon what basis covered entities can determine which registries or collections are ''legitimate'' and how the confidentiality of the registry information will be protected. Commenters did not suggest methods for ''validating'' these private registry programs, and no such methods currently exist at the federal level. It is unknown whether any states have such a program. Broadening the exemption could provide a loophole for private data collections for inappropriate

purposes or uses under a ''public health'' mask.

In this rule, we do not seek to make judgments as to the legitimacy of private entities' disease-specific registries or of private data collection endeavors. Rather, we establish the general terms and conditions for disclosure and use of protected health information. Under the final rule, covered entities may obtain authorization to disclose protected health information to private entities seeking to establish registries or other databases; they may disclose protected health information as required by law; or they may disclose protected health information to such entities if they meet the conditions of one of the provisions of §§ 164.510 or 164.512. We believe that the circumstances under which covered entities may disclose protected health information to private entities should be limited to specified national priority purposes, as reflected through the FDA requirements or directives listed in § 164.512(b)(iii), and to enable recalls, repairs, or replacements of products regulated by the FDA. Disclosures by covered health care providers who are workforce members of an employer or are conducting evaluations relating to work-related injuries or illnesses or workplace surveillance also may disclose protected health information to employers of findings of such evaluations that are necessary for the employer to comply with requirements under OSHA and related laws.

Comment: Several commenters said that the NPRM did not indicate how to distinguish between public health data collections and government health data systems. They suggested eliminating proposed § 164.510(g) on disclosures and uses for government health data systems, because they believed that such disclosures and uses were adequately covered by proposed § 164.510(b) on public health.

Response: As discussed below, we agree with the commenters who suggested that the proposed provision that would have permitted disclosures to government health data bases was overly broad, and we remove it from the final rule. We reviewed the important purposes for which some commenters said government agencies needed protected health information, and we believe that most of those needs can be met through the other categories of permitted uses and disclosures without authorization allowed under the final rule, including provisions permitting covered entities to disclose information (subject to certain limitations) to government agencies for public health, health oversight, law enforcement, and otherwise as required by law. For example, the final rule continues to allow collection of protected health information without authorization to monitor trends in the spread of infectious disease, morbidity and mortality.

Comment: Several commenters recommended expanding the scope of disclosures permissible under proposed § 164.510(b)(1)(iii), which would have allowed covered entities to disclose protected health information to private entities that could demonstrate that they were acting to comply with requirements, or at the direction, of a public health authority. These commenters said that they needed to collect individually identifiable health information in the process of drug and device development, approval, and post-market surveillance—activities that are related to, and necessary for, the FDA regulatory process. However, they noted that the specific data collections involved were not required by FDA regulations. Some commenters said that they often devised their own data collection methods, and that health care providers disclosed information to companies voluntarily for activities such as post-marketing surveillance and efficacy surveys. Commenters said they used this information to comply with FDA requirements such as reporting adverse events, filing other reports, or recordkeeping. Commenters indicated that the FDA encouraged but did not require them to establish other data collection mechanisms, such as pregnancy registries that track maternal exposure to drugs and the outcomes.

Accordingly, several commenters recommended modifying proposed § 164.510(b) to allow covered entities to disclose protected health information without authorization to manufacturers registered with the FDA to manufacture, distribute, or sell a prescription drug, device, or biological product, in connection with post-marketing safety and efficacy surveillance or for the entity to obtain information about the drug, device, or product or its use. One commenter suggested including in the regulation an illustrative list of examples of FDA-related requirements, and stating in the preamble that all activities taken in furtherance of compliance with FDA regulations are ''public health activities.''

Response: We recognize that the FDA conducts or oversees many activities that are critical to help ensure the safety or effectiveness of the many products it regulates. These activities include, for example, reporting of adverse events, product defects and problems; product tracking; and post-marketing surveillance. In addition, we believe that removing defective or harmful products from the market is a critical national priority and is an important tool in FDA efforts to promote the safety and efficacy of the products it regulates. We understand that in most cases, the FDA lacks statutory authority to require product recalls. We also recognize that the FDA typically does not conduct recalls, repairs, or product replacement surveillance directly, but rather, that it relies on the private entities it regulates to collect data, notify patients when applicable, repair and replace products, and undertake other activities to promote the safety and effectiveness of FDA-regulated products.

We believe, however, that modifying the NPRM to allow disclosure of protected health information to private entities as part of any data-gathering activity related to a drug, device, or biological product or its use, or for any activity that is consistent with, or that appears to promote objectives specified, in FDA regulation would represent an inappropriately broad exception to the general requirement to obtain authorization prior to disclosure. Such a change could allow, for example, drug companies to collect protected health information without authorization to use for the purpose of marketing pharmaceuticals. We do not agree that all activities taken to promote compliance with FDA regulations represent public health activities as that term is defined in this rule. In addition, we believe it would not be appropriate to include in the regulation text an ''illustrative list'' of requirements ''related to'' the FDA. The regulation text and preamble list the FDA-related activities for which we believe disclosure of protected health information to private entities without authorization is warranted.

We believe it is appropriate to allow disclosure of protected health information without authorization to private entities only: For purposes that the FDA has, in effect, identified as national priorities by issuing regulations or express directions requiring such disclosure; or if such disclosure is necessary for a product recall. For example, we believe it is appropriate to allow covered health care providers to disclose to a medical device manufacturer recalling defective heart valves the names and last known addresses of patients in whom the provider implanted the valves. Thus, in the final rule, we allow covered entities to disclose protected health information to entities subject to FDA jurisdiction for the following activities: To report adverse events (or similar reports with

respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations, 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 of product recalls, withdrawals, or other problems); or to conduct post-marketing surveillance to comply with requirements or at the direction of the FDA. The preamble above provides further detail on the meaning of some of the terms in this list. Covered entities may disclose protected health information to entities for activities other than those described above only as required by law; with authorization; or if permissible under another section of this rule.

We understand that many private registries, such as pregnancy registries, currently obtain patient authorization for data collection. We believe the approach of § 164.512(b) strikes an appropriate balance between the objective of promoting patient privacy and control over their health information and the objective of allowing private entities to collect data that ultimately may have important public health benefits.

Comment: One commenter remarked that our proposal may impede fetal/infant mortality and child fatality reviews.

Response: The final rule permits a covered entity to disclose protected health information to a public health authority authorized by law to conduct public health activities, including the collection of data relevant to death or disease, in accordance with § 164.512(b). Such activities may also meet the definition of ''health care operations.'' We therefore do not believe this rule impedes these activities.

Comment: Several comments requested that the final regulation clarify that employers be permitted to use and/or disclose protected health information pursuant to the requirements of the Occupational Safety and Health Act and its accompanying regulations (''OSHA''). A few comments asserted that the regulation should not only permit employers to use and disclose protected health information without first obtaining an authorization consistent with OSHA requirements, but also permit them to use and disclose protected health information if the use or disclosure is consistent with the spirit of OSHA. One commenter supported the permissibility of these types of uses and disclosures, but warned that the regulation should not grant employers unfettered access to the entire medical record of employees for the purpose of meeting OSHA requirements. Other commenters noted that OSHA not only requires disclosures to the Occupational Safety and Health Administration, but also to third parties, such as employers and employee representatives. Thus, this comment asked HHS to clarify that disclosures to third parties required by OSHA are also permissible under the regulation.

Response: Employers as such are not covered entities under HIPAA and we generally do not have authority over their actions. When an employer has a health care component, such as an on-site medical clinic, and the components meets the requirements of a covered health care provider, health plan or health care clearinghouse, the uses and disclosures of protected health information by the health care component, including disclosures to the larger employer entity, are covered by this rule and must comply with its provisions.

A covered entity, including a covered health care provider, may disclose protected health information to OSHA under § 164.512(a), if the disclosure is required by law, or if the disclosure is a discretionary one for public health activities, under § 164.512(b). Employers may also request employees to provide authorization for the employer to obtain protected health information from covered entities to conduct analyses of work-related health issues. See § 164.508.

We also permit covered health care providers who provide health care as a workforce member of an employer or at the request of an employer to disclose protected health information to the employer concerning work-related injuries or illnesses or workplace medical surveillance in situations where the employer has a duty to keep records on or act on such information under the OSHA or similar laws. We added this provision to ensure that employers are able to obtain the information that they need to meet federal and state laws designed to promote safer and healthier workplaces. These laws are vital to protecting the health and safety of workers and we permit specified covered health care providers to disclose protected health information as necessary to carry out these purposes.

Comment: A few comments suggested that the final regulation clarify how it would interact with existing and pending OSHA requirements. One of these comments requested that the Secretary delay the effective date of the regulation until reviews of existing requirements are complete.

Response: As noted in the ''Relationship to Other Federal Laws'' section of the preamble, we are not undertaking a complete review of all existing laws with which covered entities might have to comply. Instead we have described a general framework under which such laws may be evaluated. We believe that adopting national standards to protect the privacy of individually identifiable health information is an urgent national priority. We do not believe that it is appropriate to delay the effective date of this regulation.

Comment: One commenter asserted that the proposed regulation conflicted with the OSHA regulation requirement that when a designated representative (to whom the employee has already provided a written authorization to obtain access) requests a release form for access to employee medical records, the form must include the purpose for which the disclosure is sought, which the proposed privacy regulation does not require.

Response: We do not agree that this difference creates a conflict for covered entities. If an employer seeks to obtain a valid authorization under § 164.508, it may add a purpose statement to the authorization so that it complies with OSHA's requirements and is a valid authorization under § 164.508 upon which a covered entity may rely to make a disclosure of protected health information to the employer.

Comment: One commenter stated that access to workplace medical records by the occupational medical physicians is fundamental to workplace and community health and safety. Access is necessary whether it is a single location or multiple sites of the same company, such as production facilities of a national company located throughout the country.

Response: We permit covered health care providers who provide health care as a workforce member of an employer or at the request of an employer to disclose protected health information to the employer concerning work-related injuries or illnesses or workplace medical surveillance, as described in this paragraph. Information obtained by an employer under this paragraph would be available for it to use, consistent with other laws and regulations, as it chooses and throughout the national company. We do not regulate uses or disclosures of individually identifiable health

information by employers acting as employers.

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

The NPRM did not include a paragraph specifically addressing covered entities' disclosures of protected health information regarding victims of abuse, neglect, or domestic violence. Rather, the NPRM addressed disclosures about child abuse pursuant to proposed § 164.510(b), which would have allowed covered entities to report child abuse to a public health authority or to another appropriate authority authorized by law to receive reports of child abuse or neglect. We respond to comments regarding victims of domestic violence or abuse throughout the final rule where relevant. (See responses to comments on §§ 164.502(g), 164.510(b), 164.512(f)(3), 164.522, and 164.524.)

Comment: Several commenters urged us to require that victims of domestic violence be notified about requests for or disclosures of protected health information about them, so that victims could take safety precautions.

Response: We agree that, in balancing the burdens on covered entities from such a notification requirement against the benefits to be gained, victims of domestic abuse merit heightened concern. For this reason, we generally require covered entities to inform the individual when they disclose protected health information to authorized government authorities. As the Family Violence Prevention Fund has noted in its *Health Privacy Principles for Protecting Victims of Domestic Violence* (October 2000), victims of domestic violence and abuse sometimes are subject to retaliatory violence. By informing a victim of abuse or domestic violence of a disclosure to law enforcement or other authorities, covered entities give victims the opportunity to take appropriate safety precautions. See the above preamble discussion of § 164.512(c) for more detail about the requirements for disclosing protected health information about victims of domestic violence.

Comment: Some commenters argued that a consent requirement should apply at a minimum to disclosures involving victims of crime or victims of domestic violence.

Response: We agree, and we modify the proposed rule to require covered entities to obtain an individual's agreement prior to disclosing protected health information in most instances involving victims of a crime or of abuse, neglect, or domestic violence. See the above preamble discussions of § 164.512(c), on disclosures about victims of abuse, neglect, or domestic violence, and § 164.512(f)(3), on disclosures to law enforcement about crime victims.

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

Comment: A couple of commenters supported the NPRM's approach to health oversight. Several other commenters generally supported the NPRM's approach to disclosure of protected health information for national priority purposes, and they recommended some clarification regarding disclosure for health oversight. Two commenters recommended clarifying in the final rule that disclosure is allowed to all federal, state, and local agencies that use protected health information to carry out legally mandated responsibilities.

Response: The final rule permits disclosures to public agencies that meet the definition of a health oversight agency and for oversight of the particular areas described in the statute. Section 164.512(a) of the final rule permits disclosures that are required by law. As discussed in the responses to comments of § 164.512(a), we do not in the final rule permit disclosures merely authorized by other laws that do not fit within the other public policy purposes recognized by the rule.

Comment: One commenter recommended clarifying in the final rule that covered entities are not required to establish business partner contracts with health oversight agencies or public health authorities to release individually identifiable information to them for purposes exempt from HIPAA and sanctioned by state law.

Response: The final rule does not require covered entities to establish business associate contracts with health oversight agencies when they disclose protected health information to these agencies for oversight purposes.

Comment: Two commenters recommended clarifying in the regulation text that the health oversight section does not create a new right of access to protected health information.

Response: We agree and include such a statement in the preamble of § 164.512(d) of the final rule.

Comment: Several commenters were concerned that the proposed oversight section allowed but did not require disclosure of protected health information to health oversight agencies for oversight activities.

Response: This rule's purpose is to protect the privacy of individually identifiable health information. Except to enforce the rule and to establish individuals' right to access their own protected health information (see § 164.502(a)(2)), we do not require disclosure of protected health information to any person or entity. We allow such disclosure for situations in which other laws require disclosure.

Comment: Some commenters were concerned that the NPRM would have allowed health oversight agencies to re-use and redisclose protected health information to other entities, and they were particularly concerned about re-disclosure to and re-use by law enforcement agencies. One commenter believed that government agencies would use the label of health oversight to gain access to protected health information from covered entities—thereby avoiding the procedural requirements of the law enforcement section (proposed § 164.510(f)) and subsequently would turn over information to law enforcement officials. Thus, these groups were concerned that the potential for oversight access to protected health information under the rule to become the ''back door'' to law enforcement access to such information.

Based on their concerns, these commenters recommended establishing a general prohibition on the re-use and re-disclosure of protected health information obtained by health oversight agencies in actions against individuals. One health plan expressed general concern about re-disclosure among all of the public agencies covered in the proposed § 164.510. It recommended building safeguards into the rule to prevent information gathered for one purpose (for example, public health) from being used for another purpose (such as health oversight).

Many of the commenters concerned about re-disclosure of protected health information obtained for oversight purposes said that if the Secretary lacked statutory authority to regulate oversight agencies' re-disclosure of protected health information and the re-use of this information by other agencies covered in proposed § 164.510, the President should issue an Executive Order barring such re-disclosure and re-use. One of these groups specified that the Executive Order should bar re-use and re-disclosure of protected health information in actions against individuals.

In contrast, some commenters advocated information-sharing between law enforcement and oversight agencies. Most of these commenters recognized that the NPRM would have allowed re-use and re-disclosure of protected health information from oversight to law

enforcement agencies, and they supported this approach.

Response: We believe that the language we have added to the rule, at § 164.512(d)(2) and the corresponding explanation in the preamble, to clarify the boundary between disclosures for health oversight and for law enforcement purposes should partially address the concern expressed by some that oversight agencies will be the back door for access by law enforcement. In situations when the individual is the subject of an investigation or activity and the investigation or activity is not related to health care fraud, the requirements for disclosure to law enforcement must be met, and an oversight agency cannot request the information under its more general oversight authority.

We acknowledge, however, that there will be instances under the rule when a health oversight agency (or a law enforcement agency in its oversight capacity) that has obtained protected health information appropriately will be able to redisclose the information to a law enforcement agency for law enforcement purposes. Under HIPAA, we have the authority to restrict re-disclosure of protected health information only by covered entities. Re-disclosures by public agencies such as oversight agencies are not within the purview of this rule. We support the enactment of comprehensive privacy legislation that would govern such public agencies' re-use and re-disclosure of this information. Furthermore, in an effort to prevent health oversight provisions from becoming the back door to law enforcement access to protected health information, the President is issuing an Executive Order that places strict limitations on the use of protected health information gathered in the course of an oversight investigation for law enforcement activities. For example, such use will be subject to review by the Deputy Attorney General.

Comment: Several commenters recommended modifying the proposed oversight section to require health oversight officials to justify and document their need for identifiable information.

Response: We encourage covered entities to work with health oversight agencies to determine the scope of information needed for health oversight inquiries. However, we believe that requiring covered entities to obtain extensive documentation of health oversight information needs could compromise health oversight agencies' ability to complete investigations, particularly when an oversight agency is investigating the covered entity from which it is seeking information.

Comment: Several commenters believed that health oversight activities could be conducted without access to individually identifiable health information. Some of these groups recommended requiring information provided to health oversight agencies to be de-identified to the extent possible.

Response: We encourage health oversight agencies to use de-identified information whenever possible to complete their investigations. We recognize, however, that in some cases, health oversight agencies need identifiable information to complete their investigations. For example, as noted in the preamble to the NPRM, to determine whether a hospital has engaged in fraudulent billing practices, it may be necessary to examine billing records for a set of individual cases. Similarly, to determine whether a health plan is complying with federal or state health care quality standards, it may be necessary to examine individually identifiable health information in comparison with such standards. Thus, to allow health oversight agencies to conduct the activities that are central to their mission, the final rule does not require covered entities to de-identify protected health information before disclosing it to health oversight organizations.

Comment: One commenter recommended requiring whistleblowers, pursuant to proposed § 164.518(a)(4) of the NPRM, to raise the issue of a possible violation of law with the affected covered entity before disclosing such information to an oversight agency, attorney, or law enforcement official.

Response: We believe that such a requirement would be inappropriate, because it would create the potential for covered entities that are the subject of whistleblowing to take action to evade law enforcement and oversight action.

Comment: One commenter recommended providing an exemption from the proposed rule's requirements for accounting for disclosures when such disclosures were for health oversight purposes.

Response: We recognize that in some cases, informing individuals that their protected health information has been disclosed to a law enforcement official or to a health oversight agency could compromise the ability of law enforcement and oversight officials to perform their duties appropriately. Therefore, in the final rule, we retain the approach of proposed § 164.515 of the NPRM. Section 164.528(a)(2) of the final rule states that an individual's right to receive an accounting of disclosures to a health oversight agency, law enforcement official, or for national security or intelligence purposes may be temporarily suspended for the time specified by the agency or official. As described in § 164.528(a)(2), for such a suspension to occur, the agency or official must provide the affected covered entity with a written request stating that an accounting to the individual would be reasonably likely to impede the agency's activity. The request must specify the time for which the suspension is required. We believe that providing a permanent exemption to the right to accounting for disclosures for health oversight purposes would fail to ensure that individuals are sufficiently informed about the extent of disclosures of their protected health information.

Comment: One commenter recommended making disclosures to health oversight agencies subject to a modified version of the NPRM's proposed three-part test governing disclosure of protected health information to law enforcement pursuant to an administrative request (as described in proposed § 164.510(f)(1)).

Response: We disagree that it would be appropriate to apply the procedural requirements for law enforcement to health oversight. We apply more extensive procedural requirements to law enforcement disclosures than to disclosures for health oversight because we believe that law enforcement investigations more often involve situations in which the individual is the subject of the investigation (and thus could suffer adverse consequences), and we believe that it is appropriate to provide greater protection to individuals in such cases. Health oversight involves investigations of institutions that use health information as part of business functions, or of individuals whose health information has been used to obtain a public benefit. These circumstances justify broader access to information.

Overlap Between Law Enforcement and Oversight

Comment: Some commenters expressed concern that the NPRM's provisions permitting disclosures for health oversight and disclosures for law enforcement overlapped, and that the overlap could create confusion among covered entities, members of the public, and government agencies. The commenters identified particular factors that could lead to confusion, including that (1) the phrase ''criminal, civil, or administrative proceeding'' appeared in the definitions of both law enforcement

and oversight; (2) the examples of oversight agencies listed in the preamble included a number of organizations that also conduct law enforcement activities; (3) the NPRM addressed the issue of disclosures to investigate health care fraud in the law enforcement section (§ 164.510(f)(5)), yet health care fraud investigations are central to the mission of some health care oversight agencies; (4) the NPRM established more stringent rules for disclosure of protected health information pursuant to an administrative subpoena issued for law enforcement than for disclosure pursuant to an oversight agency's administrative subpoena; and (5) the 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.

Some commenters said that covered entities would be confused by the overlap between law enforcement and oversight and that this concern would lead to litigation over which rules should apply when an entity engaged in more than one of the activities listed under the exceptions in proposed § 164.510. Other commenters believed that covered entities could manipulate the NPRM's ambiguities in their favor, claim that the more stringent law enforcement disclosure rules always should apply, and thereby delay investigations. A few comments suggested that the confusion could be clarified by making the regulation text consistent with the preamble, by stating that when agencies conducting both law enforcement and oversight seek protected health information as part of their oversight activities, the oversight rules would apply.

Response: We agree that the boundary between disclosures for health oversight and disclosures for law enforcement proposed in the NPRM could have been more clear. Because many investigations, particularly investigations involving public benefit programs, have both health oversight and law enforcement aspects to them, and because the same agencies often perform both functions, drawing any distinction between the two functions is necessarily difficult. For example, traditional law enforcement agencies, such as the Federal Bureau of Investigation, have a significant role in health oversight. At the same time, traditional health oversight agencies, such as federal Offices of Inspectors General, often participate in criminal investigations.

To clarify the boundary between law enforcement and oversight for purposes of complying with this rule, we add new language in the final rule, at § 164.512(d)(2). This section indicates that health oversight activities do not include an investigation or activity in which the individual is the subject of the investigation or activity and the investigation or activity does not arise out of and is not directly related to health care fraud. In this rule, we describe investigations involving suspected health care fraud as investigations related to: (1) The receipt of health care; (2) a claim for public benefits related to health; or (3) qualification for, or receipt of public benefits or services where a patient's health is integral to the claim for public benefits or services. In such cases, where the individual is the subject of the investigation and the investigation does not relate to health care fraud, identified as investigations regarding issues (a) through (c), the rules regarding disclosure for law enforcement purposes (see § 164.512(f)) apply.

Where the individual is not the subject of the activity or investigation, or where the investigation or activity relates to health care fraud, a covered entity may make a disclosure pursuant to § 164.512(d)(1), allowing uses and disclosures for health oversight activities. 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 health plan, the health plan may disclose protected health information to the PWBA under the health oversight rules.

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 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).

We also recognize that sections 201 and 202 of HIPAA, which established a federal Fraud and Abuse Control Program and the Medicare Integrity Program, identified health care fraud-fighting as a critical national priority. Accordingly, under the final rule, in joint law enforcement/oversight investigations involving suspected health care fraud, the health oversight disclosures apply, even if the individual also is the subject of the investigation.

We also recognize that in some cases, health oversight agencies may conduct joint investigations with other oversight agencies involved in investigating claims for benefits unrelated to health. For example, in some cases, a state Medicaid agency may be working with officials of the Food Stamps program to investigate suspected fraud involving Medicaid and Food Stamps. While this issue was not raised specifically in the comments, we add new language (§ 164.512(d)(3)) to provide guidance to covered entities in such situations. Specifically, we clarify that if a health oversight investigation is conducted in conjunction with an oversight activity related to a claim for benefits unrelated to health, the joint activity or investigation is considered health oversight for purposes of the rule, and the covered entities may disclose protected health information pursuant to the health oversight provisions.

Comment: An individual commenter recommended requiring authorization for disclosure of patient records in fraud investigations, unless the individual was the subject or target of the investigation. This commenter recommended requiring a search warrant for cases in which the individual was the subject and stating that fraud investigators should have access to the minimum necessary patient information.

Response: As described above, we recognize that in some cases, activities include elements of both law enforcement and health oversight. Because we consider both of these activities to be critical national priorities, we do not require covered entities to obtain authorization for disclosure of protected health information to law enforcement or health oversight agencies—including those oversight activities related to health care fraud. We believe that investigations involving health care fraud represent health oversight rather than law enforcement. Accordingly, as indicated above, we remove proposed § 164.510(f)(5)(i) from the law enforcement section of the proposed rule and clarify that all disclosures of protected health information for health oversight are permissible without authorization. As discussed in greater detail in § 164.514, the final rule's minimum necessary standard applies to disclosures under § 164.512 unless the disclosure is required by law under § 164.512(a).

Comment: A large number of commenters expressed concern about the potential for health oversight agencies to become, in effect, the ''back door'' for law enforcement access to such information. The commenters suggested that health oversight agencies could use their relatively unencumbered access to protected health information to circumvent the more stringent process requirements that otherwise would apply to disclosures for law enforcement purposes. These commenters urged us to prohibit health oversight agencies from re-disclosing protected health information to law enforcement.

Response: As indicated above, we do not intend for the rule's permissive approach to health oversight or the absence of specific documentation to permit the government to gather large amounts of protected health information for purposes unrelated to health oversight as defined in the rule, and we do not intend for these oversight provisions to serve as a ''back door'' for law enforcement access to protected health information. While we do not have the statutory authority to regulate law enforcement and oversight agencies' re-use and re-disclosure of protected health information, we strongly support enactment of comprehensive privacy legislation that would govern public agencies' re-use and re-disclosure of this information. Furthermore, in an effort to prevent health oversight provisions from becoming the back door to law enforcement access to protected health information, the President is issuing an Executive Order that places strict limitations on the use of protected health information gathered in the course of an oversight investigation for law enforcement activities.

Comment: One commenter asked us to allow the requesting agency to decide whether a particular request for protected health information was for law enforcement or oversight purposes.

Response: As described above, we clarify the overlap between law enforcement disclosures and health oversight disclosures based on the privacy and liberty interests of the individual (whether the individual also is the subject of the official inquiry) and the nature of the public interest (whether the inquiry relates to health care fraud or to another potential violation of law). We believe it is more appropriate to establish these criteria than to leave the decision to the discretion of an agency that has a stake in the outcome of the investigation.

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

Comment: A few commenters suggested that the final rule not permit disclosures without an authorization for judicial and administrative proceedings.

Response: We disagree. Protected health information is necessary for a variety of reasons in judicial and administrative proceedings. Often it may be critical evidence that may or may not be about a party. Requiring an authorization for all such disclosures would severely impede the review of legal and administrative claims. Thus, we have tried to balance the need for the information with the individual's privacy. We believe the approach described above provides individuals with the opportunity to object to disclosures and provides a mechanism through which their privacy interests are taken into account.

Comment: A few commenters sought clarification about the interaction between permissible disclosures for judicial and administrative proceedings, law enforcement, and health oversight.

Response: In the final rule, we state that the provision permitting disclosures without an authorization for judicial and administrative proceedings does not supersede other provisions in § 164.512 that would otherwise permit or restrict the use or disclosure of protected health information. Additionally, in the descriptive preamble of § 164.512, we provide further explanation of how these provisions relate to one another.

Comments: Many commenters urged the Secretary to revise the rule to state that it does not preempt or supersede existing rules and statutes governing judicial proceedings, including rules of evidence, procedure, and discovery. One commenter asserted that dishonest health care providers and others should not be able to withhold their records by arguing that state subpoena and criminal discovery statutes compelling disclosure are preempted by the privacy regulation. Other commenters maintained that there is no need to replace providers' current practice, which typically requires either a signed authorization from the patient or a subpoena to release medical information.

Response: These comments are similar to many of the more general preemption comments we received. For a full discussion of the Secretary's response on preemption issues, see part 160—subpart B.

Comment: One commenter stated that the proposed rule creates a conflict with existing rules and statutes governing judicial proceedings, including rules of evidence and discovery. This commenter stated that the rule runs afoul of state judicial procedures for enforcement of subpoenas that require judicial involvement only when a party seeks to enforce a subpoena.

Response: We disagree with this comment. The final rule permits covered entities to disclose protected health information for any judicial or administrative procedure in response to a subpoena, discovery request, or other lawful process if the covered entity has received satisfactory assurances that the party seeking the disclosure has made reasonable efforts to ensure that the individual has been given notice of the request or has made reasonable efforts to secure a qualified protective order from a court or administrative tribunal. A covered entity may disclose protected health information in response to a subpoena, discovery request, or other lawful process without a satisfactory assurance if it has made reasonable efforts to provide the individual with such notice or to seek a qualified protected order itself. These rules do not require covered entities or parties seeking the disclosure of protected health information to involve the judiciary; they may choose the notification option rather than seeking a qualified protective order.

Many states have already enacted laws that incorporate these concepts. In California, for instance, an individual must be given ten days notice that his or her medical records are being subpoenaed from a health care provider and state law requires that the party seeking the records furnishes the health care provider with proof that the notice was given to the individual. In Montana, a party seeking discovery or compulsory process of medical records must give notice to the individual at least ten days in advance of serving the request on a health care provider, Service of the request must be accompanied by written certification that the procedure has been followed. In Rhode Island, an individual must be given notice that his or her medical records are being subpoenaed and notice of his or her right to object. The party serving the subpoena on the health care provider must provide written certification to the provider that: (1) This procedure has been followed, (2) twenty days have passed from the date of service, and (3) no challenge has been made to the disclosure or the court has ordered disclosure after resolution of a legal court challenge. In Washington, an individual must be given at least fourteen days from the date of service of notice that his or her health information is the subject of a

discovery request or compulsory process to obtain a protective order. The notice must identify the health care provider from whom the information is sought, specify the health care information that is sought, and the date by which a protective order must be obtained in order to prevent the provider from disclosing the information.

Comment: A few commenters expressed concern that the rule would place unnecessary additional burdens on health care providers because when they receive a request for disclosure in connection with an administrative or judicial procedure, they would have to determine whether the litigant's health was at issue before they made the disclosure. A number of commenters complained that this requirement would make it too easy for litigants to obtain protected health information. One commenter argued that litigants should not be able to circumvent state evidentiary rules that would otherwise govern disclosure of protected health information simply upon counsel's statement that the other party's medical condition or history is at issue.

Other commenters, however, urged that disclosure without authorization should be permitted whenever a patient places his or her medical condition or history at issue and recommended requiring the request for information to include a certification to this effect. Only if another party to litigation has raised a medical question, do these commenters believe a court order should be required. Similarly, one commenter supported a general requirement that disclosure without authorization be permitted only with a court order unless the patient has placed his or her physical or mental condition at issue.

Response: We agree with the concerns expressed by several commenters about this provision and have eliminated this requirement from the final rule.

Comment: A number of commenters stated that the proposed rule should be modified to permit disclosure without authorization pursuant to a lawful subpoena. One commenter argued that the provision would limit the scope of the Inspector General's subpoena power for judicial and administrative proceedings to information concerning a litigant whose health condition or history is at issue, and would impose a requirement that the Inspector General provide a written certification to that effect. Other commenters stated that the proposed rule would seriously impair the ability of state agencies to conduct administrative hearings on physician licensing and disciplinary matters. These commenters stated that current practice is to obtain information using subpoenas.

Other commenters argued that disclosure of protected health information for judicial and administrative proceedings should require a court order and/or judicial review unless the subject of the information consents to disclosure. These commenters believed that an attorney's certification should not be considered sufficient authority to override an individual's privacy, and that the proposed rule made it too easy for a party to litigation to obtain information about the other party.

Response: As a general matter, we agree with these comments. As noted, the final rule deletes the provision that would permit a covered entity to disclose protected health information pursuant to an attorney's certification that the individual is a party to the litigation and has put his or her medical condition at issue. Under the final rule, covered entities may disclose protected health information in response to a court or administrative order, provided that only the protected health information expressly authorized by the order is disclosed. Covered entities may also disclose protected health information in response to a subpoena, discovery request, or other lawful process without a court order, but only if the covered entity receives satisfactory assurances that the party seeking disclosure has made reasonable efforts to ensure that the individual has been notified of the request or that reasonable efforts have been made by the party seeking the information to secure a qualified protective order. Additionally, a covered entity may disclose protected health information in response to a subpoena, discovery request, or other lawful process without a satisfactory assurance if it makes reasonable efforts to provide the individual with such notice or to seek a qualified protected order itself.

We also note that the final rule specifically provides that nothing in Subchapter C should be construed to diminish the authority of any Inspector General, including authority provided in the Inspector General Act of 1978.

Comment: A number of commenters expressed concern that the proposed rule would not permit covered entities to introduce material evidence in proceedings in which, for example, the provisions of an insurance contract are at issue, or when a billing or payment issue is presented. They noted that although the litigant may be the owner of an insurance policy, he or she may not be the insured individual to whom the health information pertains. In addition, they stated that the medical condition or history of a deceased person may be at issue when the deceased person is not a party.

Response: We disagree. Under the final rule, a covered entity may disclose protected health information without an authorization pursuant to a court or administrative order. It may also disclose protected health information with an authorization for judicial or administrative proceedings in response to a subpoena, discovery request, or other lawful process without a court order, if the party seeking the disclosure provides the covered entity with satisfactory assurances that it has made reasonable efforts to ensure that the individual has been notified of the request or to seek a qualified protective order. Additionally, a covered entity may disclose protected health information in response to a subpoena, discovery request, or other lawful process without a satisfactory assurance if it makes reasonable efforts to provide the individual with such notice or to seek a qualified protected order itself. Therefore, a party may obtain the information even if the subject of the information is not a party to the litigation or deceased.

Comment: A few commenters argued that disclosure of protected health information should be limited only to those cases in which the individual has consented or a court order has been issued compelling disclosure.

Response: The Secretary believes that such an approach would impose an unreasonable burden on covered entities and the judicial system and that greater flexibility is necessary to assure that the judicial and administrative systems function smoothly. We understand that even those states that have enacted specific statutes to protect the privacy of health information have not imposed requirements as strict as these commenters would suggest.

Comment: Many commenters asked that the final rule require the notification of the disclosure be provided to the individual whose health information is subject to disclosure prior to the disclosure as part of a judicial or administrative proceeding. Most of these commenters also asked that the rule require that the individual who is the subject of a disclosure be given an opportunity to object to the disclosure. A few commenters suggested that patients be given ten days to object before requested information may be disclosed and recommend that the rule require the requester to provide a certification that notice has been provided and that ten days have passed

with no objection from the subject of the information. Some commenters suggested that if a subpoena for disclosure is not accompanied by a court order, the covered entities be prohibited from disclosing protected health information unless the individual has been given notice and an opportunity to object. Another commenter recommended requiring, in most circumstances, notice and an opportunity to object before a court order is issued and requiring the requestor of information to provide a signed document attesting the date of notification and forbid disclosure until ten days after notice is given.

Response: We agree that in some cases the provision of notice with an opportunity to object to the disclosure is appropriate. Thus, in the final rule we provide that a covered entity may disclose protected health information in response to a subpoena, discovery request or other lawful process that is not accompanied by a court order if it receives satisfactory assurance from the party seeking the request that the requesting party has made a good faith attempt to provide written notice to the individual that includes sufficient information about the litigation or proceeding to permit the individual to raise an objection to the court or administrative tribunal and that the time for the individual to raise objections has elapsed (and that none were filed or all have been resolved). Covered entities may make reasonable efforts to provide such notice as well.

In certain instances, however, the final rule permits covered entities to disclose protected health information for judicial and administrative proceedings without notice to the individual if the party seeking the request has made reasonable efforts to seek a qualified protective order, as described in the rule. A covered entity may also make reasonable efforts to seek a qualified protective order in order to make the disclosure. Additionally, a covered entity may disclose protected health information for judicial and administrative proceedings in response to an order of a court or administrative tribunal provided that the disclosure is limited to only that information that is expressly authorized by the order. The Secretary believes notice is not necessary in these instances because a court or administrative tribunal is in the best position to evaluate the merits of the arguments of the party seeking disclosure and the party who seeks to block it before it issues the order and that imposing further procedural obstacles before a covered entity may honor that disclosure request is unnecessary.

Comment: Many commenters urged the Secretary to require specific criteria for court and administrative orders. Many of these commenters proposed that a provision be added to the rule that would require court and administrative orders to safeguard the disclosure and use of protected health information. These commenters urged that the information sought must be relevant and material, as specific and narrowly drawn as reasonably practicable, and only disclosed if de-identified information could not reasonably be used.

Response: The Secretary's authority is limited to covered entities. Therefore, we do not impose requirements on courts and administrative tribunals. However, we note that the final rule limits the permitted disclosures by covered entities in court or administrative proceedings to only that information which is specified in the order from a court or an administrative body should provide a degree of protection for individuals from unnecessary disclosure.

Comment: Several commenters asked that the ''minimum necessary'' standard not apply to disclosures made pursuant to a court order because individuals could then use the rule to contest the scope of discovery requests. However, many other commenters recommended that the rule permit disclosure only of information ''reasonably necessary'' to respond to a subpoena. These commenters raised concerns with applying the ''minimum necessary'' standard in judicial and administrative proceedings, but did not believe the holder of protected health information should have blanket authority to disclose all protected health information. Some of the commenters urged that disclosure of any information about third parties that may be included in the medical records of another person— for example, the HIV status of a partner—be prohibited. Finally, some commenters disagreed with the proposed rule because it did not require covered entities to evaluate the validity of subpoenas and discovery requests to determine whether these requests ask for the ''minimum necessary'' or ''reasonably necessary'' amount of information.

Response: Under the final rule, if the disclosure is pursuant to an order of a court or administrative tribunal, covered entities may disclose only the protected health information expressly authorized by the order. In these instances, a covered entity is not required to make a determination whether or not the order might otherwise meet the minimum necessary requirement.

If the disclosure is pursuant to a satisfactory assurance from the party seeking the disclosure, at least a good faith attempt has been made to notify the individual in writing of the disclosure before it is made or the parties have sought a qualified protective order that prohibits them from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which the information was requested and that the information will be returned to the covered entity or destroyed at the end of the litigation or the proceeding. Alternatively, the covered entity may seek such notice or qualified protective order itself. This approach provides the individual with protections and places the burden on the parties to resolve their differences about the appropriateness and scope of disclosure as part of the judicial or administrative procedure itself before the order is issued, rather than requiring the covered entity to get involved in evaluating the merits of the dispute in order to determine whether or not the particular request is appropriate or too broad. In these cases, the covered entity must disclose only the protected health information that is the minimum amount necessary to achieve the purpose for which the information is sought.

We share the concern of the commenters that covered entities should redact any information about third parties before disclosing an individual's protected health information. During the fact-finding stage of our consideration of revisions to the proposed rule, we discussed this issue with representatives of covered entities. Currently, information about third parties is sometimes redacted by medical records personnel responding to requests for information. In particular, information regarding HIV status is treated with special sensitivity by these professionals. Although we considered including a special provision in the final rule prohibiting such disclosure, we decided that the revisions made to the proposed rule would provide sufficient protection. By restricting disclosure of protected health information to only that information specified in a court or administrative order or released pursuant to other types of lawful process only if the individual had notice and an opportunity to object or if the information was subject to a protective order, individuals who are concerned about disclosure of information concerning third parties will have the opportunity to raise that

issue prior to the request for disclosure being presented to the covered entity. We are reluctant to put the covered entity in the position of having to resolve disputes concerning the type of information that may be disclosed when that dispute should more appropriately be settled through the judicial or administrative procedure itself.

Comment: One commenter asked that the final regulation clarify that a court order is not required when disclosure would otherwise be permitted under the rule. This commenter noted that the preamble states that the requirement for a court order would not apply if the disclosure would otherwise be permitted under the rule. For example, disclosures of protected health information pursuant to administrative, civil, and criminal proceedings relating to ''health oversight'' are permitted, even if no court or administrative orders have been issued. However, the commenter was concerned that this principle only appeared in the preamble and not in the rule itself.

Response: Section 164.512(e)(4) of the final regulation contains this clarification.

Comment: One commenter was concerned that the rule is unclear as to whether governmental entities are given a special right to ''use'' protected health information that private parties do not have under the proposed regulation or whether governmental entities that seek or use protected health information are treated the same as private parties in their use of such information. This commenter urged that we clarify our intent regarding the use of protected health information by governmental entities.

Response: Generally governmental entities are treated the same as private entities under the rule. In a few clearly defined cases, a special rule applies. For instance, under § 164.504(e)(3), when a covered entity and its business associate are both governmental entities, they may enter into a memorandum of understanding or adopt a regulation with the force and effect of law that incorporates the requirements of a business associate contract, rather than having to negotiate a business associate contract itself.

Comment: One commenter recommended that final rule state that information developed as part of a quality improvement or medical error reduction program may not be disclosed under this provision. The commenter explained that peer review information developed to identify and correct systemic problems in delivery of care must be protected from disclosure to allow a full discussion of the root causes of such events so they may be identified and addressed. According to the commenter, this is consistent with peer review protections afforded this information by the states.

Response: The question of whether or not such information should be protected is currently the subject of debate in Congress and in the states. It would be premature for us to adopt a position on this issue until a clear consensus emerges. Under the final rule, no special protection against disclosure is provided for peer review information of the type the commenter describes. However, unless the request for disclosure fits within one of the categories of permitted or required disclosures under the regulation, it may not be disclosed. For instance, if disclosure of peer review information is required by another law (such as Medicare or a state law), covered entities subject to that law may disclose protected health information consistent with the law.

Comment: One commenter stated that the requirements of this section are in conflict with Medicare contractor current practices, as defined by the HCFA Office of General Counsel and suggested that the final rule include more specific guidelines.

Response: Because the commenter failed to indicate the nature of these conflicts, we are unable to respond.

Comment: One commenter stated that the rule should require rather than permit disclosure pursuant to court orders.

Response: Under the statutory framework adopted by Congress in HIPAA, a presumption is established that the data contained in an individual's medical record belongs to the individual and must be protected from disclosure to third parties. The only instance in which covered entities holding that information *must* disclose it is if the individual requests access to the information himself or herself. In the final rule (as in the proposed rule), covered entities *may* use or disclose protected health information under certain enumerated circumstances, but are not required to do so. We do not believe that this basic principle should be compromised merely because a court order has been issued. Consistent with this principle, we provide covered entities with the flexibility to deal with circumstances in which the covered entity may have valid reasons for declining to release the protected health information without violating this regulation.

Comment: One commenter noted that in some states, public health records are not subject to discovery, and that the proposed rule would not permit disclosure of protected health information pursuant to court order or subpoena if the disclosure is not allowed by state law. The commenter requested clarification as to whether a subpoena in a federal civil action would require disclosure if a state law prohibiting the release of public health records existed.

Response: As explained above, the final rule permits, but does not require, disclosure of protected health information pursuant to a court order. Under the applicable preemption provisions of HIPAA, state laws relating to the privacy of medical information that are more stringent than the federal rules are not preempted. To the extent that an applicable state law precludes disclosure of protected health information that would otherwise be permitted under the final rule, state law governs.

Comment: A number of commenters expressed concern that the proposed rule would negatively impact state and federal benefits programs, particularly social security and workers' compensation. One commenter requested that the final rule remove any possible ambiguity about application of the rule to the Social Security Administration's (SSA) evidence requests by permitting disclosure to all administrative level of benefit programs. In addition, several commenters stated that requiring SSA or states to provide the covered entity holding the protected health information with an individual's consent before it could disclose the information would create a huge administrative and paperwork burden with no added value to the individual. In addition, several other commenters indicated that states that make disability determinations for SSA also support special accommodation for SSA's determination process. They expressed concern that providers will narrowly interpret the HIPAA requirements, resulting in significant increases in processing time and program costs for obtaining medical evidence (especially purchased consultative examinations when evidence of record cannot be obtained). A few commenters were especially concerned about the impact on states and SSA if the final rule were to eliminate the NPRM's provision for a broad consent for ''all evidence from all sources.''

Some commenters also note that it would be inappropriate for a provider to make a minimum necessary determination in response to a request from SSA because the provider usually will not know the legal parameters of SSA's programs, or have access to the

individual's other sources of evidence. In addition, one commenter urged the Secretary to be sensitive to these concerns about delay and other negative impacts on the timely determination of disability by SSA for mentally impaired individuals.

Response: Under the final rule, covered entities may disclose protected health information pursuant to an administrative order so the flow of protected health information from covered entities to SSA and the states should not be disrupted.

Although some commenters urged that special rules should be included for state and federal agencies that need protected health information, the Secretary rejects that suggestion because, wherever possible, the public and the private sectors should operate under the same rules regarding the disclosure of health information. To the extent the activities of SSA constitute an actual administrative tribunal, covered entities must follow the requirements of § 164.512(e), if they wish to disclose protected health information to SSA in those circumstances. Not all administrative inquiries are administrative tribunals, however. If SSA's request for protected health information comes within another category of permissible exemptions, a covered entity, following the requirements of the applicable section, may disclose the information to SSA. For example, if SSA seeks information for purposes of health oversight, a covered entity that wishes to disclose the information to SSA may do so under § 164.512(d) and not § 164.512(e). If the disclosure does not come within one of the other permissible disclosures would a covered entity need to meet the requirements of § 164.512(e). If the SSA request does not come within another permissible disclosure, the agency will be treated like anyone else under the rules.

The Secretary recognizes that even under current circumstances, professional medical records personnel do not always respond unquestioningly to an agency's request for health information. During the fact finding process, professionals charged with managing provider response to requests for protected health information indicated to us that when an agency's request for protected health information is over broad, the medical records professional will contact the agency and negotiate a more limited request. In balancing the interests of individuals against the need of governmental entities to receive protected health information, we think that applying the minimum necessary standard is appropriate and that covered entities should be responsible for ensuring that they disclose only that protected health information that is necessary to achieve the purpose for which the information is sought.

Comment: In a similar vein, one commenter expressed concern that the proposed rule would adversely affect the informal administrative process usually followed in processing workers' compensation claims. Using formal discovery is not always possible, because some programs do not permit it. The commenter urged that the final rule must permit administrative agencies, employers, and workers' compensation carriers to use less formal means to obtain relevant medical evidence while the matter is pending before the agency. This commenter asked that the rule be revised to permit covered entities to disclose protected health information without authorization for purposes of federal or state benefits determinations at all levels of processing, from the initial application through continuing disability reviews.

Response: If the disclosure is required by a law relating to workers' compensation, a covered entity may disclose protected health information as authorized by and to the extent necessary to comply with that law under § 164.512(l). If the request for protected health information in connection with a workers' compensation claim is part of an administrative proceeding, a covered entity must meet the requirements set forth in § 164.512(e), and discussed above, before disclosing the information. As noted, one permissible manner by which a covered entity may disclose protected health information under § 164.512(e) is if the party seeking the disclosure makes reasonable efforts to provide notice to the individual as required by this provision. Under this method, the less formal process noted by the commenter would not be disturbed. Covered entity may disclose protected health information in response to other types of requests only as permitted by this regulation.

Section 164.512(f)—Disclosures for Law Enforcement Purposes

General Comments on Proposed § 164.510(f)

Comment: Some commenters argued that current law enforcement use of protected health information was legitimate and important. These commenters cited examples of investigations and prosecutions for which protected health information is needed, from white collar insurance fraud to violent assault, to provide incriminating evidence or to exonerate a suspect, to determine what charges are warranted and for bail decisions. For example, one commenter argued that disclosure of protected health information for law enforcement purposes should be exempt from the rule, because the proposed regulation would hamper Drug Enforcement Administration investigations. A few commenters argued that effective law enforcement requires early access to as much information as possible, to rule out suspects, assess severity of criminal acts, and for other purposes. A few commenters noted the difficulties criminal investigators and prosecutors face when fighting complex criminal schemes. In general, these commenters argued that all disclosures of protected health information to law enforcement should be allowed, or for elimination of the process requirements proposed in § 164.510(f)(1).

Response: The importance and legitimacy of law enforcement activities are beyond question, and they are not at issue in this regulation. We permit disclosure of protected health information to law enforcement officials without authorization in some situations precisely because of the importance of these activities to public safety. At the same time, individuals' privacy interests also are important and legitimate. As with all the other disclosures of protected health information permitted under this regulation, the rules we impose attempt to balance competing and legitimate interests.

Comment: Law enforcement representatives stated that law enforcement agencies had a good track record of protecting patient privacy and that additional restrictions on their access and use of information were not warranted. Some commenters argued that no new limitations on law enforcement access to protected health information were necessary, because sufficient safeguards exist in state and federal laws to prevent inappropriate disclosure of protected health information by law enforcement.

Response: Disclosure of protected health information by law enforcement is not at issue in this regulation. Law enforcement access to protected health information in the first instance, absent any re-disclosure by law enforcement, impinges on individuals' privacy interests and must therefore be justified by a public purpose that outweighs individuals' privacy interests.

We do not agree that sufficient safeguards already exist in this area. We are not aware of, and the comments did

not provide, evidence of a minimum set of protections for individuals relating to access by law enforcement to their protected health information. Federal and state laws in this area vary considerably, as they do for other areas addressed in this final rule. The need for standards in this area is no less critical than in the other areas addressed by this rule.

Comment: Many commenters argued that no disclosures of protected health information should be made to law enforcement (absent authorization) without a warrant issued by a judicial officer after a finding of probable cause. Others argued that a warrant or subpoena should be required prior to disclosure of protected health information unless the disclosure is for the purposes of identifying a suspect, fugitive, material witness, or missing persons, as described in proposed § 164.510(f)(2). Some commenters argued that judicial review prior to release of protected health information to law enforcement should be required absent the exigent and urgent circumstances identified in the NPRM in § 164.510(f)(3) and (5), or absent ''a compelling need'' or similar circumstances.

Response: In the final rule, we attempt to match the level of procedural protection for privacy required by this rule with the nature of the law enforcement need for access, the existence of other procedural protections, and individuals' privacy interests. Where other rules already impose procedural protections, this rule generally relies on those protections rather than imposing new ones. Thus, where access to protected health information is granted after review by an independent judicial officer (such as a court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer), no further requirements are necessary. Similarly, because information disclosed to a grand jury is vital to law enforcement purposes and is covered by secrecy protection, this rule allows disclosure with no further process.

We set somewhat stricter standards for disclosure of protected health information pursuant to administrative process, such as administrative subpoenas, summonses, and civil or authorized investigative demands. In these cases, the level of existing procedural protections is lower than for judicially-approved or grand jury disclosures. We therefore require a greater showing, specifically, the three-part test described in § 164.512(f)(1)(ii), before the covered entity is permitted to release protected health information. Where the information to be disclosed is about the victim of a crime, privacy interests are heightened and we require the victim's agreement prior to disclosure in most instances.

In the limited circumstances where law enforcement interests are heightened, we allow disclosure of protected health information without prior legal process or agreement, but we impose procedural protections such as limits on the information that may lawfully be disclosed, limits on the circumstances in which the information may be disclosed, and requirements for verifying the identity and authority of the person requesting the disclosures. For example, in some cases law enforcement officials may seek limited but focused information needed to obtain a warrant. A witness to a shooting may know the time of the incident and the fact that the perpetrator was shot in the left arm, but not the identity of the perpetrator. Law enforcement would then have a legitimate need to ask local emergency rooms whether anyone had presented with a bullet wound to the left arm near the time of the incident. Law enforcement may not have sufficient information to obtain a warrant, but instead would be seeking such information. In such cases, when only limited identifying information is disclosed and the purpose is solely to ascertain the identity of a person, the invasion of privacy would be outweighed by the public interest. For such circumstances, we allow disclosure of protected health information in response to a law enforcement inquiry where law enforcement is seeking to identify a suspect, fugitive, material witness, or missing person, but allow only disclosure of a limited list of information.

Similarly, it is in the public interest to allow covered entities to take appropriate steps to protect the integrity and safety of their operations. Therefore, we permit covered entities on their own initiative to disclose to law enforcement officials protected health information for this purpose. However, we limit such disclosures to protected health information that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity.

We shape the rule's provisions with respect to law enforcement according to the limited scope of our regulatory authority under HIPAA, which applies only to the covered entities and not to law enforcement officials. We believe the rule sets the correct standards for when an exception to the rule of non-disclosure is appropriate for law enforcement purposes. There may be advantages, however, to legislation that applies the appropriate standards directly to judicial officers, prosecutors in grand juries, and to those making administrative or other requests for protected health information, rather than to covered entities. These advantages could include measures to hold officials accountable if they seek or receive protected health information contrary to the legal standard. In Congressional consideration of law enforcement access, there have also been useful discussions of other topics, such as limits on re-use of protected health information gathered in the course of health oversight activities. The limitations on our regulatory authority provide additional reason to support comprehensive medical privacy legislation.

Comment: A few commenters cited existing sanctions for law enforcement officials who violate the rights of individuals in obtaining evidence, ranging from suppression of that evidence to monetary penalties, and argued that such sanctions are sufficient to protect patients' privacy interests.

Response: After-the-fact sanctions are important, but they are effective only when coupled with laws that establish the ground rules for appropriate behavior. That is, a sanction applies only where some other rule has been violated. This regulation sets such basic ground rules. Further, under the HIPAA statutory authority, we cannot impose sanctions on law enforcement officials or require suppression of evidence. We must therefore rely on rules that regulate disclosure of protected health information by covered entities in the first instance.

Comment: Several commenters argued that disclosure of protected health information under § 164.510(f) should be mandatory, not just permitted. Others argued that we should mandate disclosure of protected health information in response to Inspector General subpoenas. A few commenters argued that we should require all covered entities to include disclosure of protected health information to law enforcement in their required notice of privacy practices.

Response: The purpose of this regulation is to protect individuals' privacy interests, consistent with other important public activities. Other laws set the rules governing those public activities, including when health information is necessary for their effective operation. See discussion of § 164.512(a).

Comment: Some commenters questioned whether the Secretary had statutory authority to directly or indirectly impose new procedural or substantive requirements on otherwise lawful legal process issued under existing federal and state rules. They argued that, while the provisions are imposed on ''covered entities,'' the rule would result in law enforcement officials being compelled to modify current practices to harmonize them with the requirements this rule imposes on covered entities. A number of state law enforcement agencies argued that the rule would place new burdens on state administrative subpoenas and requests that are intrusive in state functions. At least one commenter argued that the requirement for prior process places unreasonable restrictions on the right of the states to regulate law enforcement activities.

Response: This rule regulates the ability of health care clearinghouses, health plans, and covered health care providers to use and disclose health information. It does not regulate the behavior of law enforcement officials or the courts, nor does it prevent states from regulating law enforcement officials. All regulations have some effects on entities that are not directly regulated. We have considered those effects in this instance and have determined that the provisions of the rule are necessary to protect the privacy of individuals.

Comment: One commenter argued that state licensing boards should be exempt from restrictions placed on law enforcement officials, because state licensing and law enforcement are different activities.

Response: Each state's law determines what authorities are granted to state licensing boards. Because state laws differ in this regard, we cannot make a blanket determination that state licensing officials are or are not law enforcement officials under this regulation. We note, however, that the oversight of licensed providers generally is included as a health oversight activity at § 164.512(d).

Relationship to Existing Rules and Practices

Comment: Many commenters expressed concern that the proposed rule would have expanded current law enforcement access to protected health information. Many commenters said that the NPRM would have weakened their current privacy practices with respect to law enforcement access to health records. For example, some of the commenters arguing that a warrant or subpoena should be required prior to disclosure of protected health information unless the disclosure is for the purposes of identifying a suspect, fugitive, material witness, or missing persons, did so because they believed that such a rule would be consistent with current state law practices.

Response: This regulation does not expand current law enforcement access to protected health information. We do not mandate any disclosures of protected health information to law enforcement officials, nor do we make lawful any disclosures of protected health information which are unlawful under other rules and regulations. Similarly, this regulation does not describe a set of ''best practices.'' Nothing in this regulation should cause a covered entity to change practices that are more protective of privacy than the floor of protections provided in this regulation.

This regulation sets forth the minimum practices which a covered entity must undertake in order to avoid sanctions under the HIPAA. We expect and encourage covered entities to exercise their judgment and professional ethics in using and disclosing health information, and to continue any current practices that provide privacy protections greater than those mandated in this regulation.

Comment: Many commenters asserted that, today, consent or judicial review always is required prior to release of protected health information to law enforcement; therefore, they said that the proposed rule would have lessened existing privacy protections.

Response: In many situations today, law enforcement officials lawfully obtain health information absent any prior legal process and absent exigent circumstances. The comments we received on the NPRM, both from law enforcement and consumer advocacy groups, describe many such situations. Moreover, this rule sets forth minimum privacy protections and does not preempt more stringent, pre-existing standards.

Comment: Some commenters argued that health records should be entitled to at least as much protection as cable subscription records and video rental records.

Response: We agree. The Secretary, in presenting her initial recommendations on the protection of health information to the Congress in 1997, stated that, ''When Congress looked at the privacy threats to our credit records, our video records, and our motor vehicle records, it acted quickly to protect them. It is time to do the same with our health care records' (Testimony of Donna E. Shalala, Secretary, U. S. Department of Health and Human Services, before the Senate Committee on Labor & Human Resources, September 11, 1997). However, the limited jurisdiction conferred on us by the HIPAA does not allow us to impose such restrictions on law enforcement officials or the courts.

Comment: At least one commenter argued that the regulation should allow current routine uses for law enforcement under the Privacy Act.

Response: This issue is discussed in the ''Relationship to Other Federal Laws'' preamble discussion of the Privacy Act.

Comment: A few commenters expressed concern that people will 8be less likely to provide protected health information for public health purposes if they fear the information could be used for law enforcement purposes.

Response: This regulation does not affect law enforcement access to records held by public health authorities, nor does it expand current law enforcement access to records held by covered entities. These agencies are for the most part not covered entities under HIPAA. Therefore, this regulation should not reduce current cooperation with public health efforts.

Relationship to Other Provisions of This Regulation

Comment: Several commenters pointed out an unintended interaction between proposed §§ 164.510(f) and 164.510(n). Because proposed § 164.510(n), allowing disclosures mandated by other laws, applied only if the disclosure would not fall into one of the categories of disclosures provided for in § 164.510 (b)–(m), disclosures of protected health information mandated for law enforcement purposes by other law would have been preempted.

Response: We agree, and in the final rule we address this unintended interaction. It is not our intent to preempt these laws. To clarify the interaction between these provisions, in the final rule we have specifically added language to the paragraph addressing disclosures for law enforcement that permits covered entities to comply with legal mandates, and have included a specific cross reference in the provision of the final rule that permits covered entities to make other disclosures required by law. See § 164.512(a).

Comment: Several commenters argued that, when a victim of abuse or of a crime has requested restrictions on disclosure, the restrictions should be communicated to any law enforcement officials who receive that protected health information.

Response: We do not have the authority to regulate law enforcement

use and disclosure of protected health information, and therefore we could not enforce any such restrictions communicated to law enforcement officials. For this reason, we determined that the benefits to be gained from requiring communication of restrictions would not outweigh the burdens such a requirement would place on covered entities. We expect that professional ethics will guide health care providers' communications to law enforcement officials about the welfare of victims of abuse or other crime.

Comment: Some commenters argued against imposing the ''minimum necessary'' requirement on disclosure of protected health information to law enforcement officials. Some law enforcement commenters expressed concern that the ''minimum necessary'' test could be ''manipulated'' by a covered entity that wished to withhold relevant evidence. A number of covered entities complained that they were ill-equipped to substitute their judgment for that of law enforcement for what was the minimum amount necessary, and they also argued that the burden of determining the ''minimum necessary'information should be transferred to law enforcement agencies. Some commenters argued that imposing such ''uninformed'' discretion on covered entities would delay or thwart legitimate investigations, and would result in withholding information that might exculpate an individual or might be necessary to present a defendant's case. One comment suggested that covered entities have ''immunity'' for providing too much information to law enforcement.

Response: The ''minimum necessary'' standard is discussed at § 164.514.

Comment: A few commenters asked us to clarify when a disclosure is for a ''Judicial or Administrative Proceeding'' and when it is for ''Law Enforcement'' purposes.

Response: In the final rule we have clarified that § 164.512(e) relating to disclosures for judicial or administrative proceedings does not supersede the authority of a covered entity to make disclosures under other provisions of the rule.

Use of Protected Health Information After Disclosure to Law Enforcement

Comment: Many commenters recommended that we restrict law enforcement officials' re-use and re-disclosure of protected health information. Some commenters asked us to impose such restrictions, while other commenters noted that the need for such restrictions underscores the need for legislation. Another argued for judicial review prior to release of protected health information to law enforcement because this regulation cannot limit further uses or disclosures of protected health information once it is in the hands of law enforcement agencies.

Response: We agree that there are advantages to legislation that imposes appropriate restrictions directly on the re-use and re-disclosure of protected health information by many persons who may lawfully receive protected health information under this regulation, but whom we cannot regulate under the HIPAA legislative authority, including law enforcement agencies.

Comment: A few commenters expressed concern that protected health information about persons who are not suspects may be used in court and thereby become public knowledge. These commenters urged us to take steps to minimize or prevent such protected health information from becoming part of the public record.

Response: We agree that individuals should be protected from unnecessary public disclosure of health information about them. However, we do not have the statutory authority in this regulation to require courts to impose protective orders. To the extent possible within the HIPAA statutory authority, we address this problem in § 164.512(e), Judicial and Administrative Proceedings.

Comment: Some commenters argued that evidence obtained in violation of the regulation should be inadmissible at trial.

Response: In this regulation, we do not have the authority to regulate the courts. We can neither require nor prohibit courts from excluding evidence obtain in violation of this regulation.

Comments Regarding Proposed § 164.510(f)(1), Disclosures to Law Enforcement Pursuant to Process

Comments Supporting or Opposing a Requirement of Consent or Court Order

Comment: Some commenters argued that a rule that required a court order for every instance that law enforcement sought protected health information would impose substantial financial and administrative burdens on federal and state law enforcement and courts. Other commenters argued that imposing a new requirement of prior judicial process would compromise the time-sensitive nature of many investigations.

Response: We do not impose such a requirement in this regulation.

Comment: Many commenters argued that proposed § 164.510(f)(1) would have given law enforcement officials the choice of obtaining records with or without a court order, and that law enforcement ''will choose the least restrictive means of obtaining records, those that do not require review by a judge or a prosecutor.'' Several commenters argued that this provision would have provided the illusion of barriers—but no real barriers—to law enforcement access to protected health information. A few argued that this provision would have allowed law enforcement to regulate itself.

Response: We agree with commenters that, in some cases, a law enforcement official may have discretion to seek health information under more than one legal avenue. Allowing a choice in these circumstances does not mean an absence of real limits. Where law enforcement officials choose to obtain protected health information through administrative process, they must meet the three-part test required by this regulation.

Comment: At least one commenter argued for judicial review prior to disclosure of health information because the rule will become the ''de facto'' standard for release of protected health information.

Response: We do not intend for this regulation to become the ''de facto'' standard for release of protected health information. Nothing in this regulation limits the ability of states and other governmental authorities to impose stricter requirements on law enforcement access to protected health information. Similarly, we do not limit the ability of covered entities to adopt stricter policies for disclosure of protected health information not mandated by other laws.

Comment: A few commenters expressed concern that proposed § 164.510(f)(1) would have overburdened the judicial system.

Response: The comments did not provide any factual basis for evaluating this concern.

Comment: Some commenters argued that, while a court order should be required, the standard of proof should be something other than ''probable cause.'' For example, one commenter argued that the court should apply the three-part test proposed in § 164.510(f)(1)(i)(C). Another commenter suggested a three-part test: The information is necessary, the need cannot be met with non-identifiable information, and the need of law enforcement outweighs the privacy interest of the patient. Some commenters suggested that we impose a ''clear and convincing'' standard. Another suggested that we require clear and convincing evidence that: (1) The

information sought is relevant and material to a legitimate criminal investigation; (2) the request is as specific and narrow as is reasonably practicable; (3) de-identified information, for example coded records, could not reasonably be used; (4) on balance, the need for the information outweighs the potential harm to the individuals and to patient care generally; and (5) safeguards appropriate to the situation have been considered and imposed. This comment also suggested the following as such appropriate safeguard: granting only the right to inspect and take notes; allowing copying of only certain portions of records; prohibiting removing records from the premises; placing limits on subsequent use and disclosure; and requiring return or destruction of the information at the earliest possible time.) Others said the court order should impose a ''minimum necessary'' standard.

Response: We have not revised the regulation in response to comments suggesting that we impose additional standards relating to disclosures to comply with court orders. Unlike administrative subpoenas, where there is no independent review of the order, court orders are issued by an independent judicial officer, and we believe that covered entities should be permitted under this rule to comply with them. Court orders are issued in a wide variety of cases, and we do not know what hardships might arise by imposing standards that would require judicial officers to make specific findings related to privacy.

Comment: At least one commenter argued that the proposed rule would have placed too much burden on covered entities to evaluate whether to release information in response to a court order. This comment suggested that the regulation allow disclosure to attorneys for assessment of what the covered entity should release in response to a court order.

Response: This regulation does not change current requirements on or rights of covered entities with respect to court orders for the release of health information. Where such disclosures are required today, they continue to be required under this rule. Where other law allows a covered entity to challenge a court order today, this rule will not reduce the ability of a covered entity to mount such a challenge. Under § 164.514, a covered entity will be permitted to rely on the face of a court order to meet this rule's requirements for verification of the legal authority of the request for information. A covered entity may disclose protected health information to its attorneys as needed, to perform health care operations, including to assess the covered entity's appropriate response to court orders. See definition of ''health care operations'' under § 164.501.

Comment: Many commenters argued that the regulation should prohibit disclosures of protected health information to law enforcement absent patient consent.

Response: We disagree with the comment. Requiring consent prior to any release of protected health information to a law enforcement official would unduly jeopardize public safety. Law enforcement officials need protected health information for their investigations in a variety of circumstances. The medical condition of a defendant could be relevant to whether a crime was committed, or to the seriousness of a crime. The medical condition of a witness could be relevant to the reliability of that witness. Health information may be needed from emergency rooms to locate a fleeing prison escapee or criminal suspect who was injured and is believed to have stopped to seek medical care.

These and other uses of medical information are in the public interest. Requiring the authorization of the subject prior to disclosure could make apprehension or conviction of some criminals difficult or impossible. In many instances, it would not be possible to obtain such consent, for example because the subject of the information could not be located in time (or at all). In other instances, the covered entity may not wish to undertake the burden of obtaining the consent. Rather than an across-the-board consent requirement, to protect individuals' privacy interests while also promoting public safety, we impose a set of procedural safeguards (described in more detail elsewhere in this regulation) that covered entities must ensure are met before disclosing protected health information to law enforcement officials.

In most instances, such procedural safeguards consist of some prior legal process, such as a warrant, grand jury subpoena, or an administrative subpoena that meets a three-part test for protecting privacy interests. When the information to be disclosed is about the victim of a crime, privacy interests are heightened and we require the victim's agreement prior to disclosure in most instances. In the limited circumstances where law enforcement interests are heightened and we allow disclosure of protected health information without prior legal process or agreement, the procedural protections include limits on the information that may lawfully be disclosed, the circumstances in which the information may be disclosed, and requirements for verifying the identity and authority of the person requesting the disclosures.

We also allow disclosure of protected health information to law enforcement officials without consent when other law mandates the disclosures. When such other law exists, another public entity has made the determination that law enforcement interests outweigh the individual's privacy interests in the situations described in that other law, and we do not upset that determination in this regulation.

Comment: Several commenters recommended requiring that individuals receive notice and opportunity to contest the validity of legal process under which their protected health information will be disclosed, prior to disclosure of their records to law enforcement. Some of these commenters recommended adding this requirement to provisions proposed in the NPRM, while others recommended establishing this requirement as part of a new requirement for a judicial warrant prior to all disclosures of protected health information to law enforcement. At least one of these commenters proposed an exception to such a notice requirement where notice might lead to destruction of the records.

Response: Above we discuss the reasons why we believe it is inappropriate to require consent or a judicial order prior to any release of protected health information to law enforcement. Many of those reasons apply here, and they lead us not to impose such a notice requirement.

Comment: A few commenters believed that the proposed requirements in § 164.510(f)(1) would hinder investigations under the Civil Rights for Institutionalized Persons Act (CRIPA).

Response: We did not intend that provision to apply to investigations under CRIPA, and we clarify in the final rule that covered entities may disclose protected health information for such investigations under the health oversight provisions of this regulation (see § 164.512(d) for further detail).

Comments Suggesting Changes to the Proposed Three-Part Test

Comment: Many commenters argued for changes to the proposed three-part test that would make the test more difficult to meet. Many of these urged greater, but unspecified, restrictions. Others argued that the proposed test was too stringent, and that it would have hampered criminal investigations and prosecutions. Some argued that it

was too difficult for law enforcement to be specific at the beginning of an investigation. Some argued that there was no need to change current practices, and they asked for elimination of the three-part test because it was ''more stringent'' than current practices and would make protected health information more difficult to obtain for law enforcement purposes. These commenters urged elimination of the three-part test so that administrative bodies could continue current practices without additional restrictions. Some of these argued for elimination of the three-part test for all administrative subpoenas; others argued for elimination of the three-part test for administrative subpoenas from various Inspectors General offices. A few commenters argued that the provisions in proposed § 164.510(f)(1) should be eliminated because they would have burdened criminal investigations and prosecutions but would have served ''no useful public purpose.''

Response: We designed the proposed three-part test to require proof that the government's interest in the health information was sufficiently important and sufficiently focused to overcome the individual's privacy interest. If the test were weakened or eliminated, the individual's privacy interest would be insufficiently protected. At the same time, if the test were significantly more difficult to meet, law enforcement's ability to protect the public interest could be unduly compromised.

Comment: At least one comment argued that, in the absence of a judicial order, protected health information should be released only pursuant to specific statutory authority.

Response: It is impossible to predict all the facts and circumstances, for today and into the future, in which law enforcement's interest in health information outweigh individuals' privacy interests. Recognizing this, states and other governments have not acted to list all the instances in which health information should be available to law enforcement officials. Rather, they specify some such instances, and rely on statutory, constitutional, and other limitations to place boundaries on the activities of law enforcement officials. Since the statutory authority to which the commenter refers does not often exist, many uses of protected health information that are in the public interest (described above in more detail) would not be possible under such an approach.

Comment: At least one commenter, an administrative agency, expressed concern that the proposed rule would have required its subpoenas to be approved by a judicial officer.

Response: This rule does not require judicial approval of administrative subpoenas. Administrative agencies can avoid the need for judicial review under this regulation by issuing subpoenas for protected health information only where the three-part test has been met.

Comment: Some commenters suggested alternative requirements for law enforcement access to protected health information. A few suggested replacing the three-part test with a requirement that the request for protected health information from law enforcement be in writing and signed by a supervisory official, and/or that the request ''provide enough information about their needs to allow application of the minimum purpose rule.''

Response: A rule requiring only that the request for information be in writing and signed fails to impose appropriate substantive standards for release of health information. A rule requiring only sufficient information for the covered entity to make a ''minimum necessary'' determination would leave these decisions entirely to covered entities' discretion. We believe that protection of individuals' privacy interests must start with a minimum floor of protections applicable to all. We believe that while covered entities may be free to provide additional protections (within the limits of the law), they should not have the ability to allow unjustified access to health information.

Comment: Some commenters argued that the requirement for an unspecified ''finding'' for a court order should be removed from the proposed rule, because it would have been confusing and would have provided no guidance to a court as to what finding would be sufficient.

Response: We agree that the requirement would have been confusing, and we delete this language from the final regulation.

Comment: A few commenters argued that the proposed three-part test should not be applied where existing federal or state law established a standard for issuing administrative process.

Response: It is the content of such a standard, not its mere existence, that determines whether the standard strikes an appropriate balance between individuals' privacy interests and the public interest in effective law enforcement activities. We assume that current authorities to issue administrative subpoena are all subject to some standards. When an existing standard provides at least as much protection as the three-part test imposed by this regulation, the existing standard is not disturbed by this rule. When, however, an existing standard for issuing administrative process provides less protection, this rule imposes new requirements.

Comment: Some covered entities said that they should not have been asked to determine whether the proposed three-part test has been met. Some argued that they were ill-equipped to make a judgment on whether an administrative subpoena actually met the three-part test, or that it was unfair to place the burden of making such determinations on covered entities. Some argued that the burden should have been on law enforcement, and that it was inappropriate to shift the burden to covered entities. Other commenters argued that the proposal would have given too much discretion to the record holders to withhold evidence without having sufficient expertise or information on which to make such judgments. At least one comment said that this aspect of the proposal would have caused delay and expense in the detection and prevention of health care fraud. The commenter believed that this delay and expense could be prevented by shifting to law enforcement and health care oversight the responsibility to determine whether standards have been met.

At least one commenter recommended eliminating the three-part test for disclosures of protected health information by small providers.

Some commenters argued that allowing covered entities to rely on law enforcement representation that the three-part test has been met would render the test meaningless.

Response: Because the statute does not bring law enforcement officials within the scope of this regulation, the rule must rely on covered entities to implement standards that protect individuals' privacy interests, including the three-part test for disclosure pursuant to administrative subpoenas. To reduce the burden on covered entities, we do not require a covered entity to second-guess representations by law enforcement officials that the three part test has been met. Rather, we allow covered entities to disclose protected health information to law enforcement when the subpoena or other administrative request indicates on its face that the three-part test has been met, or where a separate document so indicates. Because we allow such reliance, we do not believe that it is necessary or appropriate to reduce privacy protections for individuals who obtain care from small health care providers.

Comment: Some commenters ask for modification of the three-part test to include a balancing of the interests of law enforcement and the privacy of the individual, pointing to such provisions in the Leahy-Kennedy bill.

Response: We agree with the comment that the balancing of these interests is important in this circumstance. We designed the regulation's three-part test to accomplish that result.

Comment: At least one commenter recommended that ''relevant and material'' be changed to ''relevant,'' because ''relevant'' is a term at the core of civil discovery rules and is thus well understood, and because it would be difficult to determine whether information is ''material'' prior to seeing the documents. As an alternative, this commenter suggested explaining what we meant by ''material.''

Response: Like the term ''relevant,'' the term ''material'' is commonly used in legal standards and well understood.

Comment: At least one commenter suggested deleting the phrase ''reasonably practical'' from the second prong of the test, because, the commenter believed, it was not clear who would decide what is ''reasonably practical'' if the law enforcement agency and covered entity disagreed.

Response: We allow covered entities to rely on a representation on the face of the subpoena that the three-part test, including the ''reasonably practical'' criteria, is met. If a covered entity believes that a subpoena is not valid, it may challenge that subpoena in court just as it may challenge any subpoena that today it believes is not lawfully issued. This is true regardless of the specific test that a subpoena must meet, and is not a function of the ''reasonably practical'' criteria.

Comment: Some commenters requested elimination of the third prong of the test. One of these commenters suggested that the regulation should specify when de-identified information could not be used. Another recommended deleting the phrase ''could not reasonably be used'' from the third prong of the test, because the commenter believed it was not clear who would determine whether de-identified information ''could reasonably be used'' if the law enforcement agency and covered entity disagreed.

Response: We cannot anticipate in regulation all the facts and circumstances surrounding every law enforcement activity today, or in the future as technologies change. Such a rigid approach could not account for the variety of situations faced by covered entities and law enforcement officials, and would become obsolete over time. Thus, we believe it would not be appropriate to specify when de-identified information can or cannot be used to meet legitimate law enforcement needs.

In the final rule, we allow the covered entity to rely on a representation on the face of the subpoena (or similar document) that the three-part test, including the ''could not reasonably be used'' criteria, is met. If a covered entity believes that a subpoena is not valid, it may challenge that subpoena in court just as it may challenge today any subpoena that it believes is not lawfully issued. This is true regardless of the specific test that a subpoena must meet, and it is not a function of the ''could not reasonably be used'' criteria.

Comments Regarding Proposed § 164.510(f)(2), Limited Information for Identifying Purposes

Comment: A number of commenters recommended deletion of this provision. These commenters argued that the legal process requirements in proposed § 164.510(f)(1) should apply when protected health information is disclosed for identification purposes. At least one privacy group recommended that if the provision were not eliminated in its entirety, ''suspects'' should be removed from the list of individuals whose protected health information may be disclosed for identifying purposes. Many commenters expressed concern that this provision would allow compilation of large data bases of health information that could be use for purposes beyond those specified in this provision.

Response: We retain this provision in the final rule. We continue to believe that identifying fugitives, material witnesses, missing persons, and suspects is an important national priority and that allowing disclosure of limited identifying information for this purpose is in the public interest. Eliminating this provision—or eliminating suspects from the list of types of individuals about whom disclosure of protected health information to law enforcement is allowed—would impede law enforcement agencies'' ability to apprehend fugitives and suspects and to identify material witnesses and missing persons. As a result, criminals could remain at large for longer periods of time, thereby posing a threat to public safety, and missing persons could be more difficult to locate and thus endangered.

However, as described above and in the following paragraphs, we make significant changes to this provision, to narrow the information that may be disclosed and make clear the limited purpose of the provision. For example, the proposed rule did not state explicitly whether covered entities would have been allowed to initiate—in the absence of a request from law enforcement—disclosure of protected health information to law enforcement officials for the purpose of identifying a suspect, fugitive, material witness or missing person. In the final rule, we clarify that covered entities may disclose protected health information for identifying purposes only in response to a request by a law enforcement official or agency. A ''request by a law enforcement official or agency'' is not limited to direct requests, but also includes oral or written requests by individuals acting on behalf of a law enforcement agency, such as a media organization broadcasting a request for the public's assistance in identifying a suspect on the evening news. It includes ''Wanted'' posters, public announcements, and similar requests to the general public for assistance in locating suspects or fugitives.

Comment: A few commenters recommended additional restrictions on disclosure of protected health information for identification purposes. For example, one commenter recommended that the provision should either (1) require that the information to be disclosed for identifying purposes be relevant and material to a legitimate law enforcement inquiry and that the request be as specific and narrowly drawn as possible; or (2) limit disclosures to circumstances in which (a) a crime of violence has occurred and the perpetrator is at large, (b) the perpetrator received an injury during the commission of the crime, (c) the inquiry states with specificity the type of injury received and the time period during which treatment would have been provided, and (d) ''probable cause'' exists to believe the perpetrator received treatment from the provider.

Response: We do not agree that these additional restrictions are appropriate for disclosures of limited identifying information for purposes of locating or identifying suspects, fugitives, material witnesses or missing persons. The purpose of this provision is to permit law enforcement to obtain limited time-sensitive information without the process requirements applicable to disclosures for other purposes. Only limited information may be disclosed under this provision, and disclosure is permitted only in limited circumstances. We believe that these

safeguards are sufficient, and that creating additional restrictions would undermine the purpose of the provision and that it would hinder law enforcement's ability to obtain essential, time-sensitive information.

Comment: A number of law enforcement agencies recommended that the provision in the proposed rule be broadened to permit disclosure to law enforcement officials for the purpose of ''locating'' as well as ''identifying'' a suspect, fugitive, material witness or missing person.

Response: We agree with the comment and have changed the provision in the final rule. We believe that locating suspects, fugitives, material witnesses and missing persons is an important public policy priority, and that it can be critical to identifying these individuals. Further, efforts to locate suspects, fugitives, material witnesses, and missing persons can be at least as time-sensitive as identifying such individuals.

Comment: Several law enforcement agencies requested that the provision be broadened to permit disclosure of additional pieces of identifying information, such as ABO blood type and Rh factor, DNA information, dental records, fingerprints, and/or body fluid and tissue typing, samples and analysis. These commenters stated that additional identifying information may be necessary to permit identification of suspects, fugitives, material witnesses or missing persons. On the other hand, privacy and consumer advocates, as well as many individuals, were concerned that this section would allow all computerized medical records to be stored in a large law enforcement data base that could be scanned for matches of blood, DNA, or other individually identifiable information.

Response: The final rule seeks to strike a balance in protecting privacy and facilitating legitimate law enforcement inquiries. Specifically, we have broadened the NPRM's list of data elements that may be disclosed pursuant to this section, to include disclosure of ABO blood type and rh factor for the purpose of identifying or locating suspects, fugitives, material witnesses or missing persons. We agree with the commenters that these pieces of information are important to law enforcement investigations and are no more invasive of privacy than the other pieces of protected health information that may be disclosed under this provision.

However, as explained below, protected health information associated with DNA and DNA analysis; dental records; or typing, samples or analyses of tissues and bodily fluids other than blood (*e.g.,* saliva) cannot be disclosed for the location and identification purposes described in this section. Allowing disclosure of this information is not necessary to accomplish the purpose of this provision, and would be substantially more intrusive into individuals' privacy. In addition, we understand commenters' concern about the potential for such information to be compiled in law enforcement data bases. Allowing disclosure of such information could make individuals reluctant to seek care out of fear that health information about them could be compiled in such a data base.

Comment: Many commenters argued that proposed § 164.510(f)(2) should be deleted because it would permit law enforcement to engage in ''fishing expeditions'' or to create large data bases that could be searched for suspects and others.

Response: Some of this fear may have stemmed from the inclusion of the phrase ''other distinguishing characteristic''—which could be construed broadly—in the list of items that could have been disclosed pursuant to this section. In the final rule, we delete the phrase ''other distinguishing characteristic'' from the list of items that can be disclosed pursuant to § 164.512(f)(2). In its place, we allow disclosure of a description of distinguishing physical characteristics, such as scars, tattoos, height, weight, gender, race, hair and eye color, and the presence or absence of facial hair such as a beard or moustache. We believe that such a change, in addition to the changes described in the paragraph above, responds to commenters' concern that the NPRM would have allowed creation of a government data base of personal identifying information. Further, this modification provides additional guidance to covered entities regarding the type of information that may be disclosed under this provision.

Comment: At least one commenter recommended removing social security numbers (SSNs) from the list of items that may be disclosed pursuant to proposed § 164.510(f)(2). The commenter was concerned that including SSNs in the (f)(2) list would cause law enforcement agencies to demand that providers collect SSNs. In addition, the commenter was concerned that allowing disclosure of SSNs could lead to theft of identity by unscrupulous persons in policy departments and health care organizations.

Response: We disagree. We believe that on balance, the potential benefits from use of SSNs for this purpose outweigh the potential privacy intrusion from such use of SSNs. For example, SSNs can help law enforcement officials identify suspects are using aliases.

Comments Regarding Proposed § 164.510(f)(3), Information About a Victim of Crime or Abuse

Comment: Some law enforcement organizations expressed concern that proposed § 164.510(f)(3) could inhibit compliance with state mandatory reporting laws.

Response: We recognize that the NPRM could have preempted such state mandatory reporting laws, due to the combined impact of proposed §§ 164.510(m) and 164.510(f). As explained in detail in § 164.512(a) above, we did not intend that result, and we modify the final rule to make clear that this rule does not preempt state mandatory reporting laws.

Comment: Many commenters, including consumer and provider groups, expressed concern that allowing covered entities to disclose protected health information without authorization to law enforcement regarding victims of crime, abuse, and other harm could endanger victims, particularly victims of domestic violence, who could suffer further abuse if their abuser learned that the information had been reported. Provider groups also expressed concern about undermining provider-patient relationships. Some law enforcement representatives noted that in many cases, health care providers' voluntary reports of abuse or harm can be critical for the successful prosecution of violent crime. They argued, that by precluding providers from voluntarily reporting to law enforcement evidence of potential abuse, the proposed rule could make it more difficult to apprehend and prosecute criminals.

Response: We recognize the need for heightened sensitivity to the danger facing victims of crime in general, and victims of domestic abuse or neglect in particular. As discussed above, the final rule includes a new section (§ 164.512(c)) establishing strict conditions for disclosure of protected health information about victims of abuse, neglect, and domestic violence.

Victims of crime other than abuse, neglect, or domestic violence can also be placed in further danger by disclosure of protected health information relating to the crime. In § 164.512(f)(3) of the final rule, we establish conditions for disclosure of protected health information in these circumstances, and we make significant modifications to the proposed rule's provision for such disclosures. Under the final rule, unless a state or other

government authority has enacted a law requiring disclosure of protected health information about a victim to law enforcement officials, in most instances, covered entities must obtain the victim's agreement before disclosing such information to law enforcement officials. This requirement gives victims control over decision making about their health information where their safety could be at issue, helps promote trust between patients and providers, and is consistent with health care providers' ethical obligation to seek patient authorization whenever possible before disclosing protected health information.

At the same time, the rule strikes a balance between protecting victims and providing law enforcement access to information about potential crimes that cause harm to individuals, by waiving the requirement for agreement in two situations. In allowing covered entities to disclose protected health information about a crime victim pursuant to a state or other mandatory reporting law, we defer to other governmental bodies' judgments on when certain public policy objectives are important enough to warrant mandatory disclosure of protected health information to law enforcement. While some mandatory reporting laws are written more broadly than others, we believe that it is neither appropriate nor practicable to distinguish in federal regulations between what we consider overly broad and sufficiently focused mandatory reporting laws.

The final rule waives the requirement for agreement if the covered entity is unable to obtain the individual's agreement due to incapacity or other emergency circumstance, and (1) the law enforcement official represents that the 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 the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and (3) the covered entity determines, in the exercise of professional judgment, that the disclosure is in the individual's best interests. By allowing covered entities, in the exercise of professional judgment, to determine whether such disclosures are in the individual's best interests, the final rule recognizes the importance of the provider-patient relationship.

In addition, the final rule allows covered entities to initiate disclosures of protected health information about victims without the victim's permission to law enforcement officials only if such disclosure is required under a state mandatory reporting law. In other circumstances, plans and providers may disclose protected health information only in response to a request from a law enforcement official. We believe that such an approach recognizes the importance of promoting trust between victims and their health care providers. If providers could initiate reports of victim information to law enforcement officials absent a legal reporting mandate, victims may avoid give their providers health information that could facilitate their treatment, or they may avoid seeking treatment completely.

Comment: Many commenters believed that access to medical records pursuant to this provision should occur only after judicial review. Others believed that it should occur only with patient consent or after notifying the patient of the disclosure to law enforcement. Similarly, some commenters said that the minimum necessary standard should apply to this provision, and they recommended restrictions on law enforcement agencies' re-use of the information.

Response: As discussed above, the final rule generally requires individual agreement as a condition for disclosure of a victim's health information; this requirement provides greater privacy protection and individual control than would a requirement for judicial review. We also discuss above the situations in which this requirement for agreement may be waived, and why that is appropriate. The requirement that covered entities disclose the minimum necessary protected health information consistent with the purpose of the disclosure applies to disclosures of protected health information about victims to law enforcement, unless the disclosure is required by law. (See § 164.514 for more detail on the requirements for minimum necessary use and disclosure of protected health information.) As described above, HIPAA does not provide statutory authority for HHS to regulate law enforcement agencies' re-use of protected health information that they obtain pursuant to this rule.

Comment: A few commenters expressed concern that the NPRM would not have required law enforcement agencies' requests for protected health information about victims to be in writing. They believed that written requests could promote clarity in law enforcement requests, as well as greater accountability among law enforcement officials seeking information.

Response: We do not impose this requirement in the final rule. We believe that such a requirement would not provide significant new protection for victims and would unduly impede the completion of legitimate law enforcement investigations.

Comment: A provider group was concerned that it would be difficult for covered entities to evaluate law enforcement officials' claims that information is needed and that law enforcement activity may be necessary. Some comments from providers and individuals expressed concern that the proposed rule would have provided open-ended access by law enforcement to victims' medical records because of this difficulty in evaluating law enforcement claims of their need for the information.

Response: We modify the NPRM in several ways that reduce covered entities' decisionmaking burdens. The final rule clarifies that covered entities may disclose protected health information about a victim of crime where a report is required by state or other law, and it requires the victim's agreement for disclosure in most other instances. The covered entity must make the decision whether to disclose only in limited circumstances: when there is no mandatory reporting law; or when the victim is unable to provide agreement and 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, that the information will not be used against the victim, and that immediate law enforcement activity that depends on such information would be materially and adversely affected by waiting until the individual is able to agree to the disclosure. In these circumstances, we believe it is appropriate to rely on the covered entity, in the exercise of professional judgment, to determine whether the disclosure is in the individual's best interests. Other sections of this rule allow covered entities to reasonably rely on certain representations by law enforcement officials (see § 164.514, regarding verification,) and require disclosure of the minimum necessary protected health information for this purpose. Together, these provisions do not allow open-ended access or place undue responsibility on providers.

Comments Regarding Proposed § 164.510(f)(4), Intelligence and National Security Activities

In the final rule, we recognize that disclosures for intelligence and national security activities do not always involve

law enforcement. Therefore, we delete the provisions of proposed § 164.510(f)(4), and we address disclosures for intelligence and national security activities in § 164.512(k), on uses and disclosures for specialized government functions. Comments and responses on these issues are included below, in the comments for that section.

Comments Regarding Proposed § 164.510(f)(5), Health Care Fraud, Crimes on the Premises, and Crimes Witnessed by the Covered Entity's Workforce

Comment: Many commenters noted that proposed § 164.510(f)(5)(i), which covered disclosures for investigations and prosecutions of health care fraud, overlapped with proposed § 164.510(c) which covered disclosures for health oversight activities.

Response: As discussed more fully in § 164.512(d) of this preamble, above, we agree that proposed § 164.510(f)(5)(i) created confusion because all disclosures covered by that provision were already permitted under proposed § 164.510(c) without prior process. In the final rule, therefore, we delete proposed § 164.510(f)(5)(i).

Comment: One commenter was concerned the proposed provision would not have allowed an emergency room physician to report evidence of abuse when the suspected abuse had not been committed on the covered entity's premises.

Response: Crimes on the premises are only one type of crime that providers may report to law enforcement officials. The rules for reporting evidence of abuse to law enforcement officials are described in § 164.512(c) of the rule, and described in detail in § 164.512(c) of the preamble. An emergency room physician may report evidence of abuse if the conditions in § 164.512(c) are met, regardless of where the abuse occurred.

Comment: One commenter argued that covered entities should be permitted to disclose information that ''indicates the potential existence'' of evidence, not just information that ''constitutes evidence'' of crimes on the premises or crimes witnessed by a member of the covered entity's workforce.

Response: We agree that covered entities should not be required to guess correctly whether information will be admitted to court as evidence. For this reason, we include a good-faith standard in this provision. Covered entities may disclose information that it believes in good faith constitutes evidence of a crime on the premises. If the covered entity discloses protected health information in good faith but is wrong in its belief that the information is evidence of a violation of law, the covered entity will not be subject to sanction under this regulation.

Section 164.512(g)—Uses and Disclosures About Decedents

Coroners and Medical Examiners

Comment: We received several comments, for example, from state and county health departments, a private foundation, and a provider organization, in support of the NPRM provision allowing disclosure without authorization to coroners and medical examiners.

Response: The final rule retains the NPRM's basic approach to disclosure of coroners and medical examiners. It allows covered entities to disclose protected health information without authorization to coroners and medical examiners, for identification of a deceased person, determining cause of death, or other duties authorized by law.

Comment: In the preamble to the NPRM, we said we had considered but rejected the option of requiring covered entities to redact from individuals' medical records any information identifying other persons before disclosing the record to a coroner or medical examiner. We solicited comment on whether health care providers routinely identify other persons specifically in an individual's medical record and if so, whether in the final rule we should require health care providers to redact information about the other person before providing it to a coroner or medical examiner.

A few commenters said that medical records typically do not include information about persons other than the patient. One commenter said that patient medical records occasionally reference others such as relatives or employers. These commenters recommended requiring redaction of such information in any report sent to a coroner or medical examiner. On the other hand, other commenters said that redaction should not be required. These commenters generally based their recommendation on the burden and delay associated with redaction. In addition to citing the complexity and time involved in redaction of medical records provided to coroners, one commenter said that health plans and covered health care providers were not trained to determine the identifiable information necessary for coroners and medical examiners to do thorough investigations. Another commenter said that redaction should not be required because coroners and medical examiners needed some additional family information to determine what would be done with the deceased after their post-mortem investigation is completed.

Response: We recognize the burden associated with redacting medical records to remove the names of persons other than the patient. In addition, as stated in the preamble to the NPRM, we recognize that there is a limited time period after death within which an autopsy must be conducted. We believe that the delay associated with this burden could make it impossible to conduct a post-mortem investigation within the required time frame. In addition, we agree that health plans and covered health care providers may lack the training necessary to determine the identifiable information necessary for coroners and medical examiners to do thorough investigations. Thus, in the final rule, we do not require health plans or covered providers to redact information about persons other than the patient who may be identified in a patient's medical record before disclosing the record to a coroner or medical examiner.

Comment: One commenter said that medical records sent to coroners and medical examiners were considered their work product and thus were not released from their offices to anyone else. The commenter recommended that HHS establish regulations on how to dispose of medical records and that we create a ''no re-release'' statement to ensure that individual privacy is maintained without compromising coroners' or medical examiners' access to protected health information. The organization said that such a policy should apply regardless of whether the investigation was civil or criminal.

Response: HIPAA does not provide HHS with statutory authority to regulate coroners' or medical examiners' re-use or re-disclosure of protected health information unless the coroner or medical examiner is also a covered entity. However, we consistently have supported comprehensive privacy legislation to regulate disclosure and use of individually identifiable health information by all entities that have access to it.

Funeral Directors

Comment: One commenter recommended modifying the proposed rule to allow disclosure without authorization to funeral directors. To accomplish this change, the commenter suggested either: (1) Adding another subsection to proposed § 164.510 of the NPRM, to allow disclosure without authorization to funeral directors as needed to make arrangements for

funeral services and for disposition of a deceased person's remains; or (2) revising proposed § 164.510(e) to allow disclosure of protected health information to both coroners and funeral directors. According to this commenter, funeral directors often need certain protected health information for the embalming process, because a person's medical condition may affect the way in which embalming is performed. For example, the commenter noted, funeral directors increasingly receive bodies after organ and tissue donation, which has implications for funeral home staff duties associated with embalming.

Response: We agree with the commenter. In the final rule, we permit 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. 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.

Comment: One commenter recommended clarifying in the final rule that it does not restrict law enforcement agencies' release of medical information that many state records laws require to be reported, for example, as part of autopsy reports. The commenter recommended stating that law enforcement officials may independently gather medical information, that such information would not be covered by these rules, and that it would continue to be covered under applicable state and federal access laws.

Response: HIPAA does not give HHS statutory authority to regulate law enforcement officials' use or disclosure of protected health information. As stated elsewhere, we continue to support enactment of comprehensive privacy legislation to cover disclosure and use of all individually identifiable health information.

Comment: One commenter recommended prohibiting health plans and covered health care providers from disclosing psychotherapy notes to coroners or medical examiners.

Response: We disagree with the commenter who asserted that psychotherapy notes should only be used by or disclosed to coroners and medical examiners with authorization. Psychotherapy notes are sometimes needed by coroners and medical examiners to determine cause of death, such as in cases where suicide is suspected as the cause of death. We understand that several states require the disclosure of protected health information, including psychotherapy notes, to medical examiners and coroners. However, in the absence of a state law requiring such disclosure, we do not intend to prohibit coroners or medical examiners from obtaining the protected health information necessary to determine an individual's cause of death.

Section 164.512(h)—Uses and Disclosures for Organ Donation and Transplantation Purposes

Comment: Commenters noted that under the organ donation system, information about a patient is disclosed before seeking consent for donation from families. These commenters offered suggestions for ensuring that the system could continue to operate without consent for information sharing with organ procurement organizations and tissue banks. Commenters suggested that organ and tissue procurement organizations should be ''covered entities'' or that the procurement of organs and tissues be included in the definition of health care operations or treatment, or in the definition of emergency circumstances.

Response: We agree that organ and tissue donation is a special situation due to the need to protect potential donors' families from the stress of considering whether their loved one should be a donor before a determination has been made that donation would be medically suitable. Rather than list the entities that are ''covered entities'' or modify the definitions of health care operations and treatment or emergency circumstances to explicitly include organ procurement organizations and tissue banks, we have modified § 164.512 to permit covered entities to use or disclose protected health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissues.

Comment: Commenters asked that the rule clarify that organ procurement organizations are health care providers but not business partners of the hospitals.

Response: We agree that organ procurement organizations and tissue banks are generally not business associates of hospitals.

Disclosures and Uses for Government Health Data Systems

Comment: We received a number of comments supporting the exception for disclosure of protected health information to government health data systems. Some supporters stated a general belief that the uses of such information were important to improve and protect the health of the public. Commenters said that state agencies used the information from government health data systems to contribute to the improvement of the health care system by helping prevent fraud and abuse and helping improve health care quality, efficiency, and cost-effectiveness. Commenters asserted that state agencies take action to ensure that data they release based on these data systems do not identify individuals

We also received a large volume of comments opposed to the exception for use and disclosure of protected health information for government health data systems. Many commenters expressed general concern that the provision threatened their privacy, and many believed that their health information would be subject to abuse by government employees. Commenters expressed concern that the provision would facilitate collection of protected health information in one large, centralized government health database that could threaten privacy. Others argued that the proposed rule would facilitate law enforcement access to protected health information and could, in fact, become a database for law enforcement use.

Many commenters asserted that this provision would make individuals concerned about confiding in their health care providers. Some commenters argued that the government should not be allowed to collect individually identifiable health information without patient consent, and that the government could use de-identified data to perform the public policy analyses. Many individual commenters said that HHS lacked statutory and Constitutional authority to give the government access and control of their medical records without consent.

Many commenters believed that the NPRM language on government health data systems was too broad and would allow virtually any government collection of data to be covered. They argued that the government health data system exception was unnecessary because there were other provisions in the proposed rules providing sufficient authority for government agencies to obtain the information they need.

Some commenters were concerned that the NPRM's government health data system provisions would allow disclosure of protected health information for purposes unrelated to health care. These commenters recommended narrowing the provision to allow disclosure of protected health

information without consent to government health data systems in support of health care-related policy, planning, regulatory, or management functions. Others recommended narrowing the exception to allow use and disclosure of protected health information for government health databases only when a specific statute or regulation has authorized collection of protected health information for a specific purpose.

Response: We agree with the commenters who suggested that the proposed provision that would have permitted disclosures to government health data bases was overly broad, and we remove it from the final rule.

We reviewed the important purposes identified in the comments for government access to protected health information, and believe that the disclosures of protected health information that should appropriately be made without individuals' authorization can be achieved through the other disclosures provided for in the final rule, including provisions permitting covered entities to disclose information (subject to certain limitations) to government agencies for public health, research, health oversight, law enforcement, and otherwise as required by law. For example, the final rule continues to allow a covered entity to disclose protected health information without authorization to a public health authority to monitor trends in the spread of infectious disease, morbidity, and mortality. Under the rule's health oversight provision, covered entities can continue to disclose protected health information to public agencies for purposes such as analyzing the cost and quality of services provided by covered entities; evaluating the effectiveness of federal, state, and local public programs; examining trends in health insurance coverage of the population; and analyzing variations in access to health coverage among various segments of the population. We believe that it is better to remove the proposed provision for government health data systems generally and to rely on other, more narrowly tailored provisions in the rule to authorize appropriate disclosures to government agencies.

Comment: Some provider groups, private companies, and industry organizations recommended expanding the exception for government health data systems to include data collected by private entities. These commenters said that such an expansion would be justified, because private entities often perform the same functions as public agencies collecting health data.

Response: We eliminate the exception for government health data systems because it was over broad and the uses and disclosures we were trying to permit are permitted by other provisions. We note that private organizations may use or disclose protected health information pursuant to multiple provisions of the rule.

Comment: One commenter recommended clarifying in the final rule that the government health data system provisions apply to: (1) Manufacturers providing data to HCFA and its contractors to help the agency make reimbursement and related decisions; and to (2) third-party payors that must provide data collected by device manufacturers to HCFA to help the agency make reimbursement and related decisions.

Response: The decision to eliminate the general provision permitting disclosures to government health data systems makes this issue moot with respect to such disclosures. We note that the information used by manufacturers to support coverage determinations often is gathered pursuant to patient authorization (as part of informed consent for research) or as an approved research project. There also are many cases in which information can be de-identified before it is disclosed. Where HCFA hires a contractor to collect such protected health information, the contractor may do so under HCFA's authority, subject to the business associate provisions of this rule.

Comment: One commenter recommended stating in the final rule that de-identified information from government health data systems can be disclosed to other entities.

Response: HHS does not have the authority to regulate re-use or re-disclosure of information by agencies or institutions that are not covered entities under the rule. However, we support the policies and procedures that public agencies already have implemented to de-identify any information that they redisclose, and we encourage the continuation of these activities.

Disclosures for Payment Processes

Proposed § 164.510(j) of the NPRM would have allowed disclosure of protected health information without authorization for banking and payment processes. In the final rule, we eliminate this provision. Disclosures that would have been allowed under it, as well as comments received on proposed § 164.510(j), are addressed under § 164.501 of the final rule, under the definition of ''payment.''

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

Documentation Requirements of IRB or Privacy Board Approval of Waiver

Comment: A number of commenters argued that the proposed research requirements of § 164.510(j) exceeded the Secretary's authority under section 246(c) of HIPAA. In particular, several commenters argued that the Department was proposing to extend the Common Rule and the use of the IRB or privacy boards beyond federally-funded research projects, without the necessary authority under HIPAA to do so. One commenter stated that, ''Section 246(c) of HIPAA requires the Secretary to issue a regulation setting privacy standards for individually identifiable health information transmitted in connection with the transactions described in section 1173(a),'' and thus concluded that the disclosure of health information to researchers is not covered. Some of these commenters also argued that the documentation requirements of proposed § 164.510(j), did not shield the NPRM from having the effect of regulating research by placing the onus on covered health care providers to seek documentation that certain standards had been satisfied before providing protected health information to researchers. These commenters argued that the proposed rule had the clear and intended effect of directly regulating researchers who wish to obtain protected health information from a covered entity.

Response: As discussed above, we do not agree with commenters that the Secretary's authority is limited to individually identifiable health information transmitted in connection with the transactions described in section 1173(a) of HIPAA. We also disagree that the proposed research documentation requirements would have constituted the unauthorized regulation of researchers. The proposed requirements established conditions for the use of protected health information by covered entities for research and the disclosure of protected health information by covered entities to researchers. HIPAA authorizes the Secretary to regulate such uses and disclosures, and the final rule retains documentation requirements similar to those proposed.

Comment: Several commenters believed that the NPRM was proposing either directly or indirectly to modify the Common Rule and, therefore, stated that such modification was beyond the Secretary's authority under HIPAA. Many of these commenters arrived at this conclusion because the waiver of

authorization criteria proposed in § 164.510(j) differed from the Common Rule's criteria for the waiver of informed consent (Common Rule, § .116(d)).

Response: We do not agree that the proposed provision relating to research would have modified the Common Rule. The provisions that we proposed and provisions that we include in the final rule place conditions that must be met before a covered entity may use or disclose protected health information. Those conditions are in addition to any conditions required of research entities under the Common Rule. Covered entities will certainly be subject to laws and regulations in addition to the rule, but the rule does not require compliance with these other laws or regulations. For covered health care providers and health plans that are subject to both the final rule and the Common Rule, both sets of regulations will need to be followed.

Comment: A few commenters suggested that the Common Rule should be extended to all research, regardless of funding source.

Response: We generally agree with the commenters on the need to provide protections to all human subjects research, regardless of funding source. HIPAA, however, did not provide the Department with authority to extend the Common Rule beyond its current purview. For research that relies on the use or disclosure of protected health information by covered entities without authorization, the final rule applies the Common Rule's principles for protecting research subjects by, in most instances, requiring documentation of independent board review, and a finding that specified criteria designed to protect the privacy of prospective research subjects have been met.

Comment: A large number of commenters agreed that the research use and disclosure of protected health information should not require authorization. Of these commenters, many supported the proposed rule's approach to research uses and disclosures without authorization, including many from health care provider organizations, the mental health community, and members of Congress. Others, while they agreed that the research use and disclosure should not require authorization disagreed with the NPRM's approach and proposed alternative models.

The commenters who supported the NPRM's approach to permitting researchers access to protected health information without authorization argued that it was appropriate to apply ''Common Rule-like'' provisions to privately funded research. In addition, several commenters explicitly argued that the option to use a privacy board, in lieu of an IRB, must be maintained because requiring IRB review to include all aspects of patient privacy could diffuse focus and significantly compromise an IRB's ability to execute its primary patient protection role. Furthermore, several commenters believed that privacy board review should be permitted, but wanted equal oversight and accountability for privacy boards and IRBs.

Many other commenters agreed that the research use and disclosure should not require authorization, but disagreed with the proposed rule's approach and proposed alternative models. Several of these commenters argued that the final rule should eliminate the option for privacy board review and that all research to be subject to IRB review. These commenters stated that having separate and unequal systems to approve research based on its funding source would complicate compliance and go against the spirit of the regulations. Several of these commenters, many from patient and provider organizations, opposed the permitted use of privacy boards to review research studies and instead argued that IRB review should be required for all studies involving the use or disclosure of protected health information. These commenters argued that although privacy board requirements would be similar, they are not equitable; for example, only three of the Common Rule's six requirements for the membership of IRBs were proposed to be required for the membership on privacy boards, and there was no proposed requirement for annual review of ongoing research studies that used protected health information. Several commenters were concerned that the proposed option to obtain documentation of privacy board review, in lieu of IRB review, would perpetuate the divide in the oversight of federally-funded versus publically-funded research, rather than eliminate the differential oversight of publically-and privately-funded research, with the former still being held to a stricter standard. Some of these commenters argued that these unequal protections would be especially apparent for the disclosure of research with authorization, since under the Common Rule, IRB review of human subjects studies is required, regardless of the subject's consent, before the study may be conducted.

Response: Although we share the concern raised by commenters that the option for the documentation of privacy board approval for an alteration or waiver of authorization may perpetuate the unequal mechanisms of protecting the privacy of human research subjects for federally-funded versus publically-funded research, the final rule is limited by HIPAA to addressing only the use and disclosure of protected health information by covered entities, not the protection of human research subjects more generally. Therefore, the rule cannot standardize human subjects protections throughout the country. Given the limited scope of the final rule with regard to research, the Department believes that the option to obtain documentation of privacy board approval for an alteration or waiver of authorization in lieu of IRB approval provides covered entities with needed flexibility. Therefore, in the final rule we have retained the option for covered entities to rely on documentation of privacy board approval that specified criteria have been met.

We disagree with the rationale suggested by commenters who argued that the option for privacy board review must be maintained because requiring IRB review to include all aspects of patient privacy could diffuse focus and significantly compromise an IRB's ability to execute its primary patient protection role. For research that involves the use of individually identifiable health information, assessing the risk to the privacy of research subjects is currently one of the key risks that must be assessed and addressed by IRBs. In fact, we expect that it will be appropriate for many research organizations that have existing IRBs to rely on these IRBs to meet the documentation requirements of § 164.512(i).

Comment: One health care provider organization recommended that the IRB or privacy board mechanism of review should be applied to non-research uses and disclosures.

Response: We disagree. Imposing documentation of privacy board approval for other public policy uses and disclosures permitted by § 164.512 would result in undue delays in the use or disclosure of protected health information that could harm individuals and the public. For example, requiring that covered health care providers obtain third-party review before permitting them to alert a public health authority that an individual was infected with a serious communicable disease could cause delay appropriate intervention by a public health authority and could present a serious threat to the health of many individuals.

Comment: A number of commenters, including several members of Congress,

argued that since the research provisions in proposed § 164.510(j) were modeled on the existing system of human subjects protections, they were inadequate and would shatter public trust if implemented. Similarly, some commenters, asserted that IRBs are not accustomed to reviewing and approving utilization reviews, outcomes research, or disease management programs and, therefore, IRB review may not be an effective tool for protecting patient privacy in connection with these activities. Some of these commenters noted that proposed § 164.510(j) would exacerbate the problems inherent in the current federal human subjects protection system especially in light of the recent GAO reports that indicate the IRB system is already over-extended. Furthermore, a few commenters argued that the Common Rule's requirements may be suited for interventional research involving human subjects, but is ill suited to the archival and health services research typically performed using medical records without authorization. Therefore, these commenters concluded that extending ''Common Rule-like'' provisions to the private sector would be inadequate to protect human subjects and would result in significant and unnecessary cost increases.

Response: While the vast majority of government-supported and regulated research adheres to strict protocols and the highest ethical standards, we agree that the federal system of human subjects protections can and must be strengthened. To work toward this goal, on May 23, the Secretary announced several additional initiatives to enhance the safety of subjects in clinical trials, strengthen government oversight of medical research, and reinforce clinical researchers' responsibility to follow federal guidelines. As part of this initiative, the National Institutes of Health have undertaken an aggressive effort to ensure IRB members and IRB staff receive appropriate training in bioethics and other issues related to research involving human subjects, including research that involves the use of individually identifiable health information. With these added improvements, we believe that the federal system of human subjects protections continues to be a good model to protect the privacy of individually identifiable health information that is used for research purposes. This model of privacy protection is also consistent with the recent recommendations of both the Institute of Medicine in their report entitled, ''Protecting Data Privacy in Health Services Research,'' and the Joint Commission on Accreditation of Healthcare Organizations and the National Committee for Quality Assurance in their report entitled, ''Protecting Personal Health Information: A Framework for Meeting the Challenges in a Managed Care Environment.'' Both of these reports similarly concluded that health services research that involves the use of individually identifiable health information should undergo IRB review or review by another board with sufficient expertise in privacy and confidentiality protection.

Furthermore, it is important to recognize that the Common Rule applies not only to interventional research, but also to research that uses individually identifiable health information, including archival research and health services research. The National Bioethics Advisory Commission (NBAC) is currently developing a report on the federal oversight of human subjects research, which is expected to address the unique issues raised by non-interventional human subjects research. The Department looks forward to receiving NBAC's report, and carefully considering the Commission's recommendations. This final rule is the first step in enhancing patients' privacy and we will propose modifications to the rule if changes are warranted by the Commission's findings and recommendations.

Comment: Many commenters argued that the proposed research provision would have a chilling affect on the willingness of health plans and covered providers to participate in research because of the criminal and civil penalties that could be imposed for failing to meet the requirements that would have been required by proposed § 164.510(j). Some of these commenters cautioned, that over time, research could be severely hindered if covered entities choose not to disclose protected health information to researchers. In addition, one commenter recommended that a more reasonable approach would be to require IRB or privacy board approval only if the results of the research were to be broadly published. Another commenter expressed concern that the privacy rule could influence IRBs or privacy boards to refuse to recognize the validity of decisions by other IRBs or privacy boards and specifically recommended that the privacy rule include a preamble statement that: (1) The ''risk'' balancing consider only the risk to the patient, not the risk to the institution, and (2) add a phrase that the decision by the initial IRB or privacy board to approve the research shall be given deference by other IRBs or privacy boards. This commenter also recommended that to determine whether IRBs or privacy boards were giving such deference to prior IRB or privacy board review, HHS should monitor the disapproval rate by IRB or privacy boards conducting secondary reviews.

Response: As the largest federal sponsor of medical research, we understand the important role of research in improving our Nation's health. However, the benefits of research must be balanced against the risks, including the privacy risks, for those who participate in research. An individual's rights and welfare must never be sacrificed for scientific or medical progress. We believe that the requirements for the use and disclosure of protected health information for research without authorization provides an appropriate balance. We understand that some covered health care providers and health plans may conclude that the rule's documentation requirements for research uses and disclosures are too burdensome.

We rejected the recommendation that documentation of IRB or privacy board approval of the waiver of authorization should only be required if the research were to be ''broadly published.'' Research findings that are published in de-identified form have little influence on the privacy interests of individuals. We believe that it is the use or disclosure of individually identifiable health information to a researcher that poses the greater risk to individuals' privacy, not publication of de-identified information.

We agree with the commenters that IRB or privacy board review should address the privacy interests of individuals and not institutions. This provision is intended to protect individuals from unnecessary uses and disclosures of their health information and does not address institutional privacy.

We disagree with the comment that documentation of IRB or privacy board approval of the waiver of authorization should be given deference by other IRBs or privacy boards conducting secondary reviews. We do not believe that it is appropriate to restrict the deliberations or judgments of privacy boards, nor do we have the authority under this rule to instruct IRBs on this issue. Instead, we reiterate that all disclosures for research purposes under § 164.512(i) are voluntary, and that institutions may choose to impose more stringent requirements for any use and disclosure permitted under § 164.512.

Comment: Some commenters were concerned about the implications of proposed § 164.510(j) on multi-center research. These commenters argued that for multi-center research, researchers may require protected health information from multiple covered entities, each of whom may have different requirements for the documentation of IRB or privacy board review. Therefore, there was concern that documentation that may suffice for one covered entity, may not for another, thereby hindering multi-center research.

Response: Since § 164.512(i) establishes minimum documentation standards for covered health care providers and health plans using or disclosing protected health information for research purposes, we understand that some covered providers and health plans may choose to require additional documentation requirements for researchers. We note, however, that nothing in the final rule would preclude a covered health care provider or health plan from developing the consistent documentation requirements provided they meet the requirements of § 164.512(i).

Comment: One commenter who was also concerned that the minimum necessary requirements of proposed § 164.506(b) would negatively affect multi-center research because covered entities participating in multi-site research studies would no longer be permitted to rely upon the consent form approved by a central IRB, and nor would participating entities be permitted to report data to the researcher using the case report form approved by the central IRB to guide what data points to include. This commenter noted that the requirement that each site would need to undertake a separate minimum necessary review for each disclosure would erect significant barriers to the conduct of research and may compromise the integrity and validity of data combined from multiple sites. This commenter recommended that the Secretary absolve a covered entity of the responsibility to make its own individual minimum necessary determinations if the entity is disclosing information pursuant to an IRB or privacy board-approved protocol.

Response: The minimum necessary requirements in the final rule have been revised to permit covered entities to rely on the documentation of IRB or privacy board approval as meeting the minimum necessary requirements of § 164.514. However, we anticipate that much multi-site research, such as multi-site clinical trials, will be conducted with patients' informed consent as required by the Common Rule and FDA's protection of human subjects regulations, and that patients' authorization will also be sought for the use or disclosure of protected health information for such studies. Therefore, it should be noted that the minimum necessary requirements do not apply for uses or disclosures made with an authorization. In addition, the final rule allows a covered health care provider or health plan to use or disclose protected health information pursuant to an authorization that was approved by a single IRB or privacy board, provided the authorization met the requirements of § 164.508. The final rule does not, however, require IRB or privacy board review for the use or disclosure of protected health information for research conducted with individuals' authorization.

Comment: Some commenters believed that proposed § 164.510(j) would have required documentation of both IRB and privacy board review before a covered entity would be permitted to disclose protected health information for research purposes without an individual's authorization.

Response: This is incorrect. Section 164.512(i)(1)(i) of the final rule requires documentation of alteration or waiver approval by either an IRB or a privacy board.

Comment: Some commenters believed that the proposed rule would have required that patients be notified whenever protected health information about themselves was disclosed for research purposes.

Response: This is incorrect. Covered entities are not required to inform individuals that protected health information about themselves has been disclosed for research purposes. However, as required in § 164.520 of the final rule, the covered entity must include research disclosures in their notice of information practices. In addition, as required by § 164.528 of the rule, covered health care providers and health plans must provide individuals, upon request, with an accounting of disclosures made of protected health information about the individual.

Comment: One commenter recommended that IRB and privacy boards also be required to be accredited.

Response: While we agree that the issue of accrediting IRBs and privacy boards deserves further consideration, we believe it is premature to require covered entities to ensure that the IRB or privacy board that approves an alteration or waiver of authorization is accredited. Currently, there are no accepted accreditation standards for IRBs or privacy boards, nor a designated accreditation body. Recognizing the need for and value of greater uniformity and public accountability in the review and approval process, HHS, with support from the Office of Human Research Protection, National Institutes of Health, Food and Drug Administration, Centers for Disease Control and Prevention, and Agency for Health Care Research and Quality, has engaged the Institute of Medicine to recommend uniform performance resource-based standards for private, voluntary accreditation of IRBs. This effort will draw upon work already undertaken by major national organizations to develop and test these standards by the spring of 2001, followed by initiation of a formal accreditation process before the end of next year. Once the Department has received the Institute of Medicine's recommended accreditation standards and process for IRBs, we plan to consider whether this accreditation model would also be applicable to privacy boards.

Comment: A few commenters also noted that if both an IRB and a privacy board reviewed a research study and came to conflicting decisions, proposed § 164.510(j) was unclear about which board's decision would prevail.

Response: The final rule does not stipulate which board's decision would prevail if an IRB and a privacy board came to conflicting decisions. The final rule requires covered entities to obtain documentation that one IRB or privacy board has approved of the alteration or waiver of authorization. The covered entity, however, has discretion to request information about the findings of all IRBs and/or privacy boards that have reviewed a research proposal. We strongly encourage researchers to notify IRBs and privacy boards of any prior IRB or privacy board review of a research protocol.

Comment: Many commenters noted that the NPRM included no guidance on how the privacy board should approve or deny researchers' requests. Some of these commenters recommended that the regulation stipulate that privacy boards be required to follow the same voting rules as required under the Common Rule.

Response: We agree that the Common Rule (§ __.108(b)) provides a good model of voting procedures for privacy boards and incorporate such procedures to the extent they are relevant. In the final rule, we require that the documentation of alteration or waiver of authorization state that the alteration or waiver has been reviewed and approved by either (1) an IRB that has followed the voting requirements of the Common Rule (§ __.108(b)), or the expedited review

procedures of the Common Rule (§ __.110); or (2) unless an expedited review procedure is used, a privacy board that has reviewed the proposed research at a convened meeting 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.

Comment: A few commenters were concerned that the research provisions would be especially onerous for small non-governmental entities, furthering the federal monopoly on research.

Response: We understand that the documentation requirements of § 164.512(i), as well as other provisions in the final rule, may be more onerous for small entities than for larger entities. We believe, however, that when protected health information is to be used or disclosed for research without an individual's authorization, the additional privacy protections in § 164.512(i) are essential to reduce the risk of harm to the individual.

Comment: One commenter believed that it was paradoxical that, under the proposed rule, the disclosure of protected health information for research conducted with an authorization would have been more heavily burdened than research that was conducted without authorization, which they reasoned was far less likely to bring personal benefit to the research subjects.

Response: It was not our intent to impose more requirements on covered entities using or disclosing protected health information for research conducted with authorization than for research conducted without authorization. In fact, the proposed rule would have required only authorization as stipulated in proposed § 164.508 for research disclosures made with authorization, and would have been exempt from the documentation requirements in proposed § 164.510(j). We retain this treatment in the final rule. We disagree with the commenter who asserted that the requirements for research conducted with authorization are more burdensome for covered health care providers and plans than the documentation provisions of this paragraph.

Comment: A number of comments, mostly from the pharmaceutical industry, recommended that the final rule state that privacy boards be permitted to waive authorization only with respect to research uses of medical information collected in the course of treatment or health care operations, and not with respect to clinical research. Similarly, one commenter recommended that IRBs and privacy boards be authorized to review privacy issues only, not the entire research project. These commenters were concerned that by granting waiver authority to privacy boards and IRBs, and by incorporating the Common Rule waiver criteria into the waiver criteria included in the proposed rule, the Secretary has set the stage for privacy boards to review and approve waivers in circumstances that involve interventional research that is not subject to the Common Rule.

Response: We agree with the commenters who recommended that the final rule clarify that the documentation of IRB or privacy board approval of the waiver of authorization would be based only on an assessment of the privacy risks associated with a research study, not an assessment of all relevant risks to participants. In the final rule, we have amended the language in the waiver criteria to make clear that these criteria relate only to the privacy interests of the individual. We anticipate, however, that the vast majority of uses and disclosures of protected health information for interventional research will be made with individuals' authorization. Therefore, we expect it will be rare that a researcher will seek IRB or privacy board approval for the alteration or waiver of authorization, but seek informed consent for participation for the interventional component of the research study. Furthermore, we believe that interventional research, such as most clinical trials, could not meet the waiver criteria in the final rule (§ 164.512(i)(2)(ii)(C)), which states ''the research could not practicably be conducted without the alteration or waiver.'' If a researcher is to have direct contact with research subjects, the researcher should in virtually all cases be able to seek and obtain patients' authorization for the use and disclosure of protected health information about themselves for the research study.

Comment: A few commenters recommended that the rule explicitly state that covered entities would be permitted to rely upon an IRB or privacy boards' representation that the research proposal meets the requirements of proposed § 164.510(j).

Response: We agree with this comment. The final rule clarifies that covered health care providers and health plans are allowed to rely on an IRB's or privacy board's representation that the research proposal meets the requirements of § 164.512(i).

Comment: One commenter recommended that IRBs be required to maintain web sites with information on proposed and approved projects.

Response: We agree that it could be useful for IRBs and privacy boards to maintain web sites with information on proposed and approved projects. However, requiring this of IRBs and privacy boards is beyond the scope of our authority under HIPAA. In addition, this recommendation raises concerns that would need to be addressed, including concerns about protecting the confidentiality of research participants and propriety information that may be contained in research proposals. For these reasons, we decided not to incorporate this requirement into the final rule.

Comment: One commenter recommended that HHS collect data on research-related breaches of confidentiality and investigate existing anecdotal reports of such breaches.

Response: This recommendation is beyond HHS' legal authority, since HIPAA did not give us the authority to regulate researchers. Therefore, this recommendation was not included in the final rule.

Comment: A number of commenters were concerned that HIPAA did not give the Secretary the authority to protect information once it was disclosed to researchers who were not covered entities.

Response: The Secretary shares these commenters' concerns about the Department's limited authority under HIPAA. We strongly support the enactment of additional federal legislation to fill these crucial gaps in the Secretary's authority.

Comment: One commenter recommended that covered entities should be required to retain the IRB's or privacy board's documentation of approval of the waiver of individuals' authorization for at least six years from when the waiver was obtained.

Response: We agree with this comment and have included such a requirement in the final rule. See § 164.530(j).

Comment: One commenter recommended that whenever health information is used for research or administrative purposes, a plan is in place to evaluate whether to and how to feed patient-specific information back into the health system to benefit an individual or group of patients from whom the health information was derived.

Response: While we agree that this recommendation is consistent with the

responsible conduct of research, HIPAA did not give us the authority to regulate research. Therefore, this recommendation was not included in the final rule.

Comment: A few commenters recommended that contracts between covered entities and researcher be pursued. Comments received in favor of requiring contractual agreements argued that such a contract would be enforceable under law, and should prohibit secondary disclosures by researchers. Some of these commenters recommended that contracts between covered entities and researchers should be the same as, or modeled on, the proposed requirements for business partners. In addition, some commenters argued that contracts between covered entities and researchers should be required as a means of placing equal responsibility on the researcher for protecting protected health information and for not improperly re-identifying information.

Response: In the final rule, we have added an additional waiver criteria to require that there are adequate written assurances from the researcher that protected health information will not be re-used or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of protected health information would be permitted by this subpart. We believe that this additional waiver criteria provides additional assurance that protected health information will not be misused by researchers, while not imposing the additional burdens of a contractual requirement on covered health care providers and health plans. We were not persuaded by the comments received that contractual requirements would provide necessary additional protections, that would not also be provided by the less burdensome waiver criteria for adequate written assurance that the researcher will not re-use or disclose protected health information, with few exceptions. Our intent was to strengthen and extend existing privacy safeguards for protected health information that is used or disclosed for research, while not creating unnecessary disincentives to covered health care providers and health plans who choose to use or disclose protected health information for research purposes.

Comment: Some commenters explicitly opposed requiring contracts between covered entities and researchers as a condition of permitting the use or disclosure of protected health information for research purposes. These commenters argued that such a contractual requirement would be too onerous for covered entities and researchers and would hinder or halt important research.

Response: We agree with the arguments raised by these commenters, and thus, the final rule does not require contracts between covered entities and researchers as a condition of using or disclosing protected health information for research purposes without authorization.

Comment: A large number of commenters strongly supported requiring patient consent before protected health information could be used or disclosed, including but not limited to use and disclosure for research purposes. These commenters argued that the unconsented-to use of their medical records abridged their autonomy right to decide whether or not to participate in research. A few referenced the Nuremberg Code in support of their view, noting that the Nuremberg Code required individual consent for participation in research.

Response: We agree that it is of foremost importance that individuals' privacy rights and welfare be safeguarded when protected health information about themselves is used or disclosed for research studies. We also strongly believe that continued improvements in the nation's health requires that researchers be permitted access to protected health information without authorization in certain circumstances. Additional privacy protections are needed, however, and we have included several in the final rule. If covered entities plan to disclose protected health without individuals' authorization for research purposes, individuals must be informed of this through the covered entity's notice to patients of their information practices. In addition, before covered health care providers or health plans may use or disclose protected health information for research without authorization, they must obtain documentation that an IRB or privacy board has found that specified waiver criteria have been met, unless the research will include protected health information about deceased individuals only, or is solely for reviews that are preparatory to research.

While it is true that the first provision of the Nuremberg Code states that ''the voluntary consent of the human subject is absolutely essential,'' it is important to understand the context of this important document in the history of protecting human subjects research from harm. The Nuremberg Code was developed for the Nuremberg Military Tribunal as standards by which to judge the human experimentation conducted by the Nazis, and was one of the first documents setting forth principles for the ethical conduct of human subjects research. The acts of atrocious cruelty that the Nuremberg Code was developed to address, focused on preventing the violations to human rights and dignity that occurred in the name of ''medical advancement.'' The Code, however, did not directly address the ethical conduct of non-interventional research, such as medical records research, where the risk of harm to participants can be unlike those associated with clinical research.

We believe that the our proposed requirements for the use or disclosure of protected health information for research are consistent with the ethical principles of ''respect for persons,'' ''beneficence,'' and ''justice,'' which were established by the Belmont Report in 1978, and are now accepted as the quintessential requirements for the ethical conduct of research involving human subjects, including research using individually identifiable health information. These ethical principles formed the foundation for the requirements in the Common Rule, on which our proposed requirements for research uses and disclosures were modeled.

Comment: Many commenters recommended that the privacy rule permit individuals to opt out of having their records used for the identified ''important'' public policy purposes in § 164.510, including for research purposes. These commenters asserted that permitting the use and disclosure of their protected health information without their consent, or without an opportunity to ''opt out'' of having their information used or disclosed, abridged individuals' right to decide who should be permitted access to their medical records. In addition, one commenter argued that although the research community has been sharply critical of a Minnesota law that limits access to health records (Minnesota Statute Section 144.335 (1998)), researchers have cited a lack of response to mailed consent forms as the primary factor behind a decrease in the percentage of medical records available for research. This commenter argued that an opt-out provision would not be subject to this ''nonresponder'' problem.

Response: We believe that a meaningful right to ''opt out'' of a research study requires that individuals be contacted and informed about the study for which protected health information about themselves is being requested by a researcher. We concluded, therefore, that an ''opt out'' provision of this nature may suffer from

the same decliner bias that has been experienced by researchers who are subject to laws that require patient consent for medical records research. Furthermore, evidence on the effect of a mandatory ''opt out'' provision for medical records research is only fragmentary at this time, but at least one study has preliminarily suggested that those who refuse to consent for research access to their medical records may differ in statistically significant ways from those who consent with respect to variables such as age and disease category (SJ Jacobsen et al. ''Potential Effect of Authorization Bias on Medical Records Research.'' Mayo Clin Proc 74: (1999) 330–338). For these reasons, we disagree with the commenters who recommended that an ''opt out'' provision be included in the final rule. In the final rule, we do require covered entities to include research disclosures in their notice of information practices. Therefore, individuals who do not wish for protected health information about themselves to be disclosed for research purposes without their authorization could select a health care provider or health plan on this basis. In addition, the final rule also permits covered health care providers or health plans to agree not to disclose protected health information for research purposes, even if research disclosures would otherwise be permitted under their notice of information practices. Such an agreement between a covered health care provider or health plan and an individual would not be enforceable under the final rule, but might be enforceable under applicable state law.

Comment: Some commenters explicitly recommended that there should be no provision permitting individuals to opt out of having their information used for research purposes.

Response: We agree with these commenters for the reasons discussed above.

IRB and Privacy Board Review

Comments: The NPRM imposed no requirements for the location or sponsorship of the IRB or privacy board. One commenter supported the proposed approach to permit covered entities to rely on documentation of a waiver by a IRB or privacy board that was convened by the covered entity, the researcher, or another entity.

In contrast, a few commenters recommended that the NPRM require that the IRB or privacy board be outside of the entity conducting the research, although the rationale for these recommendations was not provided. Several industry and consumer groups alternatively recommended that the regulation require that privacy boards be based at the covered entity. These comments argued that ''if the privacy board is to be based at the entity receiving data, and that entity is not a covered entity, there will be little ability to enforce the regulation or study the effectiveness of the standards.''

Response: We agree with the comment supporting the proposed rule's provision to impose no requirements for the location or sponsorship of the IRB or privacy board that was convened to review a research proposal for the alteration or waiver of authorization criteria. In the absence of a rationale, we were not persuaded by the comments asserting that the IRB or privacy board should be convened outside of the covered entity. In addition, while we agree with the comments that asserted HHS would have a greater ability to enforce the rule if a privacy board was established at the covered entity rather than an uncovered entity, we concluded that the additional burden that such a requirement would place on covered entities was unwarranted. Furthermore, under the Common Rule and FDA's protection of human subjects regulations, IRB review often occurs at the site of the recipient researchers' institution, and it was not our intent to change this practice. Therefore, in the final rule, we continue to impose no requirements for the location or sponsorship of the IRB or privacy board.

Privacy Board Membership

Comment: Some commenters were concerned that the proposed composition of the privacy board did not adequately address potential conflicts of interest of the board members, particularly since the proposed rule would have permitted the board's ''unaffiliated'' member to be affiliated with the entity disclosing the protected health information for research purposes. To address this concern, some commenters recommended that the required composition of privacy boards be modified to require ''* * * at least one member who is not affiliated with the entity receiving or disclosing protected health information.'' These commenters believed that this addition would be more sound and more consistent with the Common Rule's requirements for the composition of IRBs. Furthermore, it was argued that this requirement would prohibit covered entities from creating a privacy board comprised entirely of its own employees.

Response: We agree with these comments. In the final rule we have revised the proposed membership for privacy board to reduce potential conflict of interest among board members. The final rule requires that documentation of alteration or waiver from a privacy board, is only valid under § 164.512(i) if the privacy board includes 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 a person who is affiliated with such entities.

Comment: One commenter recommended that privacy boards be required to include more than one unaffiliated member to address concerns about conflict of interest among members.

Response: We disagree that privacy boards should be required to include more than one unaffiliated member. We believe that the revised membership criterion for the unaffiliated member of the privacy board, and the criterion that requires that the board have no member participating in a review of any project in which the member has a conflict of interest, are sufficient to ensure that no member of the board has a conflict of interest in a research proposal under their review.

Comment: Many commenters also recommended that the membership of privacy boards be required to be more similar to that of IRBs. These commenters were concerned that privacy boards, as described in the proposed rule, would not have the needed expertise to adequately review and oversee research involving the use of protected health information. A few of these commenters also recommended that IRBs be required to have at least one member trained in privacy or security matters.

Response: We disagree with the comments asserting that the membership of privacy boards should be required be more similar to IRBs. Unlike IRBs, privacy boards only have responsibility for reviewing research proposals that involve the use or disclosure of protected health information without authorization. We agree, however, that the proposed rule may not have ensured that the privacy board had the necessary expertise to protect adequately individuals' privacy rights and interests. Therefore, in the final rule, we have modified one of the membership criteria for privacy board to require that the 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.

Comment: Two commenters recommended that IRBs and privacy

boards be required to include patient advocates.

Response: The Secretary's legal authority under HIPAA does not permit HHS to modify the membership of IRBs. Moreover, we disagree with the comments recommending that IRBs and privacy board should be required to include patient advocates. We were not persuaded that patient advocates are the only persons with the needed expertise to protect patients' privacy rights and interests. Therefore, in the final rule, we do not require that patient advocates be included as members of a privacy board. However, under the final rule, IRBs and privacy board members could include patient advocates provided they met the required membership criteria in § 164.512(i).

Comment: A few commenters requested clarification of the term ''conflict of interest'' as it pertained to the proposed rule's criteria for IRB and privacy board membership. In particular, some commenters recommended that the final rule clarify what degree of involvement in a research project by a privacy board member would constitute a conflict, thereby precluding that individual's participation in a review. One commenter specifically requested clarification about whether employment by the covered entity constituted a conflict of interest, particularly if the covered entity is receiving a financial gain from the conduct of the research.

Response: We understand that determining what constitutes conflict of interest can be complex. We do not believe that employees of covered entities or employees of the research institution requesting protected health information for research purposes are necessarily conflicted, even if those employees may benefit financially from the research. However, there are many factors that should be considered in assessing whether a member of an IRB has a conflict of interest, including financial and intellectual conflicts.

As part of a separate, but related effort to the final rule, during the summer of 2000, HHS held a conference on human subject protection and financial conflicts of interest. In addition, HHS solicited comments from the public about financial conflicts of interest associated with human subjects research for researchers, IRB members and staff, and research sponsors. The findings from the conference and the public comments received are forming the basis for guidance that HHS is now developing on financial conflicts of interest.

Privacy Training for IRB and Privacy Boards

Comment: A few commenters expressed support for training IRB members and chairs about privacy issues, recommending that such training either be required or that it be encouraged in the final rule.

Response: We agree with these comments and thus encourage institutions that administer IRBs and privacy boards to ensure that the members of these boards are adequately trained to protect the privacy rights and welfare of individuals about whom protected health information is used for research purposes. In the final rule, we require that privacy board members have 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. We believe that this criterion for privacy board membership requires that members already have the necessary knowledge or that they be trained to address privacy issues that arise in the conduct of research that involves the use of protected health information. In addition, we note that the Common Rule (§ .107(a)) already imposes a general requirement that IRB members posses adequate training and experience to adequately evaluate the research which it reviews. IRBs are also authorized to obtain the services of consultants (§ .107(f)) to provide expertise not available on the IRB. We believe that these existing requirements in the Common Rule already require that an IRB have the necessary privacy expertise.

Waiver Criteria

Comment: A large number of comments supported the proposed rule's criteria for the waiver of authorization by an IRB or privacy board.

Response: While we agree that several of the waiver criteria should be retained in the final rule, we have made changes to the waiver criteria to address some of the comments we received on specific criteria. These reason for these changes are discussed in the response to comments below.

Comment: In addition to the proposed waiver criteria, several commenters recommended that the final rule also instruct IRBs and privacy boards to consider the type of protected health information and the sensitivity of the information to be disclosed in determining whether to grant a waiver, in whole or in part, of the authorization requirements.

Response: We agree with these comments, but believe that the requirement to consider the type and sensitivity of protected health information was already encompassed by the proposed waiver criteria. We encourage and expect that IRBs and privacy boards will take into consideration the type and sensitivity of protected health information, as appropriate, in considering the waiver criteria included in the final rule.

Comment: Many commenters were concerned that the criteria were not appropriate in the context of privacy risks and recommended that the waiver criteria be rewritten to more precisely focus on the protection of patient privacy. In addition, some commenters argued that the proposed waiver criteria were redundant with the Common Rule and were confusing because they mix elements of the Common Rule's waiver criteria—some of which they argued were relevant only to interventional research. In particular, a number of commenters raised these concerns about proposed criterion (ii). Some of these commenters suggested that the word ''privacy'' be inserted before ''rights.''

Response: We agree with these comments. To focus all of the criterion on individuals' privacy interests, in the final rule, we have modified one of the proposed waiver criteria, eliminated one proposed criterion, and added an additional criterion : (1) the proposed criterion which stated, ''the waiver will not adversely affect the rights and welfare of the subjects,'' has been revised in the final rule as follows: ''the alteration or waiver will not adversely affect the privacy rights and the welfare of the individuals;'' (2) the proposed criterion which stated, ''whenever appropriate, the subjects will be provided with additional pertinent information after participation,'' has been eliminated; and (3) a criterion has been added in the final rule which states, ''there are adequate written assurances that the protected health information will not be re-used or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of protected health information would be permitted by this subpart.'' In addressing these criteria, we expect that IRBs and privacy boards will not only consider the immediate privacy interests of the individual that would arise from the proposed research study, but also the possible implications from a loss of privacy, such as the loss of employment, loss or change in cost of health insurance, and social stigma.

Comment: A number of commenters were concerned about the interaction between the proposed rule and the Common Rule. One commenter opposed the four proposed waiver criteria which differed from the Common Rule's criteria for the waiver of informed consent (§ .116(d)) on the grounds that the four criteria proposed in addition to the Common Rule's waiver criteria would apply only to the research use and disclosure of protected health information by covered entities. This commenter argued that this would lead to different standards for the protection of other kinds of individually identifiable health information used in research that will fall outside of the scope of the final rule. This commenter concluded that this inconsistency would be difficult for IRBs to administer, difficult for IRB members to distinguish, and would be ethically questionable. For these reasons, many commenters recommended that the final rule should permit the waiver criteria of the Common Rule, to be used in lieu of the waiver criteria identified in the proposed rule.

Response: We disagree with the comments recommending that the waiver criteria of the Common Rule should be permitted to be used in lieu of the waiver criteria identified in the proposed rule. The Common Rule's waiver criteria were designed to protect research subjects from all harms associated with research, not specifically to protect individuals' privacy interests. We understand that the waiver criteria in the final rule may initially cause confusion for IRBs and researchers that must attend to both the final rule and the Common Rule, but we believe that the additional waiver criteria adopted in the final rule are essential to ensure that individuals' privacy rights and welfare are adequately safeguarded when protected health information about themselves is used for research without their authorization. We agree that ensuring that the privacy rights and welfare of all human subjects—involved in all forms of research—is ethically required, and the new Office of Human Research Protection will immediately initiate plans to review the confidentiality provisions of the Common Rule.

In addition, at the request of the President, the National Bioethics Advisory Commission has begun an examination of the current federal human system for the protection of human subjects in research. The current scope of the federal regulatory protections for protecting human subjects in research is just one of the issues that will be addressed in the by the Commission's report, and the Department looks forward to receiving the Commission's recommendations.

Concerns About Specific Waiver Criteria

Comment: One commenter argued that the term ''welfare'' was vague and recommended that it be deleted from the proposed waiver of authorization criterion which stated, ''the waiver will not adversely affect the rights and welfare of the subjects.''

Response: We disagree with the comment recommending that the final rule eliminate the term ''welfare'' from this waiver criterion. As discussed in the National Bioethics Advisory Commission's 1999 report entitled, ''Research Involving Human Biological Materials: Ethical Issues and Policy Guidance,'' ''Failure to obtain consent may adversely affect the rights and welfare of subjects in two basic ways. First, the subject may be improperly denied the opportunity to choose whether to assume the risks that the research presents, and second, the subject may be harmed or wronged as a result of his or her involvement in research to which he or she has not consented * * *. Subjects' interest in controlling information about themselves is tied to their interest in, for example, not being stigmatized and not being discriminated against in employment and insurance.'' Although this statement by the Commission was made in the context of research involving human biological materials, we believe research that involves the use of protected health information similarly requires that social and psychological harms be considered when assessing whether an alteration or waiver will adversely affect the privacy rights and welfare of individuals. We believe it would be insufficient to attend only to individuals' privacy ''rights'' since some of the harms that could result from a breach of privacy, such as stigmatization, and discrimination in employment or insurance, may not be tied directly to an individuals' ''rights,'' but would have a significant impact on their welfare. Therefore, in the final rule, we have retained the term ''welfare'' in this criterion for the alteration or waiver of authorization but modified the criterion as follows to focus more specifically on privacy concerns and to clarify that it pertains to alterations of authorization: ''the alteration or waiver will not adversely affect the privacy rights and the welfare of the individual.''

Comment: A few commenters recommended that the proposed waiver criteria that stated, ''the research could not practicably be conducted without the waiver,'' be modified to eliminate the term ''practicably.'' These commenters believed that determining ''practicably'' was subjective and that its elimination would facilitate IRBs' and privacy boards' implementation of this criterion. In addition, one commenter was concerned that this term could be construed to require authorization if enough weight is given to a privacy interest, and little weight is given to cost or administrative burden. This commenter recommended that the criterion be changed to allow a waiver if the ''disclosure is necessary to accomplish the research or statistical purpose for which the disclosure is to be made.''

Response: We disagree with the comments recommending that the term ''practicability'' be deleted from this waiver criterion. We believe that an assessment of practicability is necessary to account for research that may be possible to conduct with authorization but that would be impracticable if authorization were required. For example, in research study that involves thousands of records, it may be possible to track down all potential subjects, but doing so may entail costs that would make the research impracticable. In addition, IRBs have experience implementing this criterion since it is nearly identical to a waiver criterion in the Common Rule (§ __.116(d)(3)).

We also disagree with the recommendation to change the criterion to state, ''disclosure is necessary to accomplish the research or statistical purpose for which the disclosure is to be made.'' We believe it is essential that consideration be given as to whether it would be practicable for research to be conducted with authorization in determining whether a waiver of authorization is justified. If the research could practicably be conducted with authorization, then authorization must be sought. Authorization must not be waived simply for convenience.

Therefore, in the final rule, we have retained this criterion and clarified that it also applies to alterations of authorization. This waiver criterion in the final rule states, ''the research could not practicably be conducted without the alteration or waiver.''

Comment: Some commenters argued that the criterion which stated, ''whenever appropriate, the subjects will be provided with additional pertinent information after participation,'' should be deleted. Some comments recommended that the criterion should be deleted for privacy reasons, arguing that it would be inappropriate to create a reason for the researcher to contact the individual

whose data were analyzed, without IRB review of the proposed contact as a patient intervention. Other commenters argued for the deletion of the criterion on grounds that requiring researchers to contact patients whose records were used for archival research would be unduly burdensome, while adding little to the patient's base of information. Several commenters also argued that the criterion was not pertinent to non-interventional retrospective research requiring access to archived protected health information.

In addition, one commenter asserted that this criterion was inconsistent with the Secretary's rationale for prohibiting disclosures of ''research information unrelated to treatment'' for purposes other than research. This commenter argued that the privacy regulations should not mandate that a covered entity provide information with unknown validity or utility directly to patients. This commenter recommended that a patient's physician, not the researcher, should be the one to contact a patient to discuss the significance of new research findings for that individual patient's care.

Response: Although we disagree with the arguments made by commenters recommending that this criterion be eliminated in the final rule, we concluded that the criterion was not directly related to ensuring the privacy rights and welfare of individuals. Therefore, we eliminated this criterion in the final rule.

Comment: A few commenters recommended that the criterion, which required that ''the research would be impracticable to conduct without access to and use of the protected health information,'' be deleted because it would be too subjective to be meaningful.

Response: We disagree with comments asserting that this proposed criterion would be too subjective. We believe that researchers should be required to demonstrate to an IRB or privacy board why protected health information is necessary for their research proposal. If a researcher could practicably use de-identified health information for a research study, protected health information should not be used or disclosed for the study without individuals' authorization. Therefore, we retain this criterion in the final rule. In considering this criterion, we expect IRBs and privacy boards to consider the amount of information that is needed for the study. To ensure the covered health care provider or health plan is informed of what information the IRB or privacy board has determined may be used or disclosed without authorization, the final rule also requires that the documentation of IRB or privacy board approval of the alteration or waiver describe the protected health information for which use or access has been determined to be necessary.

Comment: A large number of comments objected to the proposed waiver criterion, which stated that, ''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.'' The majority of these commenters argued that the criterion was overly subjective, and that due to its subjectivity, IRBs and privacy boards would inevitably apply it inconsistently. Several commenters asserted that this criterion was unsound in that it would impose on reviewing bodies the explicit requirement to form and debate conflicting value judgments about the relative weights of the research proposal versus an individual's right to privacy. Furthermore these commenters argued that this criterion was also unnecessary because the Common Rule already has a requirement that deals with this issue more appropriately. In addition, one commenter argued that the rule eliminate this criterion because common purposes should not override individual rights in a democratic society. Based on these arguments, these commenters recommended that this criterion be deleted.

Response: We disagree that it is inappropriate to ask IRBs and privacy boards to ensure that there is a just balance between the expected benefits and risks to individual participants from the research. As noted by several commenters, IRBs currently conduct such a balancing of risks and benefits because the Common Rule contains a similar criterion for the approval of human subjects research (§ __.111(a)(2)). However, we disagree with the comments asserting that the proposed criterion was unnecessary because the Common Rule already contains a similar criterion. The Common Rule does not explicitly address the privacy interests of research participants and does not apply to all research that involves the use or disclosure of protected health information. However, we agree that the relevant Common Rule criterion for the approval of human subjects research provides better guidance to IRBs and privacy boards for assessing the privacy risks and benefits of a research proposal. Therefore, in the final rule, we modeled the criterion on the relevant Common Rule requirement for the approval of human subjects research, and revised the proposed criterion to state: ''the privacy risks to individuals whose protected health information is to be used or disclosed are reasonable in relation to the anticipated benefits if any to the individuals, and the importance of the knowledge that may reasonably be expected to result from the research.''

Comment: One commenter asserted that as long as the research organization has adequate privacy protections in place to keep the information from being further disclosed, it is unnecessary for the IRB or privacy board to make a judgment on whether the value of the research outweighs the privacy intrusion.

Response: The Department disagrees with the assertion that adequate safeguards of protected health information are sufficient to ensure that the privacy rights and welfare of individuals are adequately protected. We believe it is imperative that there be an assessment of the privacy risks and anticipated benefits of a research study that proposes to use protected health information without authorization. For example, if a research study was so scientifically flawed that it would provide no useful knowledge, any risk to patient privacy that might result from the use or disclosure of protected health information without individuals' authorization would be too great.

Comment: A few commenters asserted that the proposed criterion requiring ''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 identifiers,'' conflicted with the regulations of the FDA on clinical record keeping (21 CFR 812.140(d)) and the International Standard Organization on control of quality records (ISO 13483, 4.16), which require that relevant data be kept for the life of a device.

In addition, one commenter asserted that this criterion could prevent follow up care. Similarly, other commenters argued that the new waiver criteria would be likely to confuse IRBs and may impair researchers' ability to go back to IRBs to request extensions of time for which samples or data can be stored if researchers are unable to anticipate future uses of the data.

Response: We do not agree with the comment that there is a conflict between either the FDA or the ISO regulations and the proposed waiver criteria in the rule. We believe that compliance with such recordkeeping requirements would be ''consistent with the conduct of research'' which is subject to such requirements. Nonetheless, to avoid any confusion, in the final rule we have added the phrase ''or such retention is

otherwise required by law'' to this waiver criterion.

We also disagree with the comments that this criterion would prevent follow up care to individuals or unduly impair researchers from retaining identifiers on data for future research. We believe that patient care would qualify as a ''health * * * justification for retaining identifiers.'' In addition, we understand that researchers may not always be able to anticipate that the protected health information they receive from a covered health care provider or health plan for one research project may be useful for the conduct of future research studies. However, we believe that the concomitant risk to patient privacy of permitting researchers to retain identifiers they obtained without authorization would undermine patient trust, unless researchers could identify a health or research justification for retaining the identifiers. In the final rule, an IRB or privacy board is not required to establish a time limit on a researcher's retention of identifiers.

Additional Waiver Criteria

Comment: A few comments recommended that there be a additional waiver criterion to safeguard or limit subsequent use or disclosure of protected health information by the researcher.

Response: We agree with these comments. In the final rule, we include a waiver criterion requiring ''there are adequate written assurances that the protected health information will not be re-used or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of protected health information would be permitted by this subpart.''

Waiving Authorization, in Whole or in Part

Comment: A few commenters requested that the final rule clarify what ''in whole or in part'' means if authorization is waived or altered.

Response: In the proposed rule, it was HHS' intent to permit IRBs and privacy boards to either waive all of the elements for authorization, or alternatively, waive only some of the elements of authorization. Furthermore, we also intended to permit IRBs and privacy boards to alter the authorization requirements. Therefore, in the final rule, we clarify that the alteration to and waiver of authorization, in whole or in part, are permitted as stipulated in § 164.512(i).

Expedited Review

Comment: One commenter asserted that the proposed rule would prohibit expedited review as permitted under the Common Rule. Many commenters supported the proposal in the rule to incorporate the Common Rule's provision for expedited review, and strongly recommended that this provision be retained in the final rule. Several of these commenters argued that the expedited review mechanism provides IRBs with the much-needed flexibility to focus volunteer-IRB members' limited resources.

Response: We agree that expedited review should be available, and included a provision permitting expedited review under specified conditions. We understand that the National Bioethics Advisory Commission is currently developing a report on the federal oversight of human subjects research, which is expected to address the Common Rule's requirements for expedited review. HHS looks forward to receiving the National Bioethics Advisory Commission's report, and will modify the provisions for expedited review in the privacy rule if changes are warranted by the Commission's findings and recommendations.

Required Signature

Comment: A few commenters asserted that the proposed requirement that the written documentation of IRB or privacy board approval be signed by the chair of the IRB or the privacy board was too restrictive. Some commenters recommended that the final rule permit the documentation of IRB or privacy board approval to be signed by persons other than the IRB or privacy board chair, including: (1) Any person authorized to exercise executive authority under IRB's or privacy board's written procedures; (2) the IRB's or privacy board's acting chair or vice chair in the absence of the chair, if permitted by IRB procedures; and (3) the covered entity's privacy official.

Response: We agree with the commenters who argued that the final rule should permit the documentation of IRB or privacy board approval to be signed by someone other than the chair of the board. In the final rule, we permit the documentation of alteration or waiver of authorization to be signed by the chair or other member, as designated by the chair of the IRB or privacy board, as applicable.

Research Use and Disclosure With Authorization

Comment: Some commenters, including several industry and consumer groups, argued that the proposed rule would establish a two-tiered system for public and private research. Privately funded research conducted with an authorization for the use or disclosure of protected health information would not require IRB or privacy board review, while publically funded research conducted with authorization would require IRB review as required by the Common Rule. Many of these commenters argued that authorization is insufficient to protect patients involved in research studies and recommended that IRB or privacy board review should be required for all research regardless of sponsor. These commenters asserted that it is not sufficient to obtain authorization, and that IRBs and privacy boards should review the authorization document, and assess the risks and benefits to individuals posed by the research.

Response: For the reasons we rejected the recommendation that we eliminate the option for privacy board review and require IRB review for the waiver of authorization, we also decided against requiring documentation of IRB or privacy board approval for research conducted with authorization. HHS strongly agrees that IRB review is essential for the adequate protection of human subjects involved in research, regardless of whether informed consent and/or individuals' authorization is obtained. In fact, IRB review may be even more important for research conducted with subjects' informed consent and authorization since such research may present greater than minimal risk to participants. However, HHS' authority under HIPAA is limited to safeguarding the privacy of protected health information, and does not extend to protecting human subjects more broadly. Therefore, in the final rule we have not required documentation of IRB or privacy board review for the research use or disclosure of protected health information conducted with individuals' authorization. As mentioned above, HHS looks forward to receiving the recommendations of the National Bioethics Advisory Commission, which is currently examining the current scope of federal regulatory protections for protecting human subjects in research as part of its overarching report on the federal oversight of human subjects protections.

Comment: Due to concern about several of the elements of authorization, many commenters recommended that the final rule stipulate that ''informed consent'' obtained pursuant to the Common Rule be deemed to meet the requirements for ''authorization.'' These commenters argued that the NPRM's

additional authorization requirements offered no additional protection to research participants but would be a substantive impediment to research.

Response: We disagree with the comments asserting that the proposed requirements for authorization for the use or disclosure of protected health information would have offered research subjects no additional privacy protection. Because the purposes of authorization and informed consent differ, the proposed rule's requirements for authorization pursuant to a request from a researcher (§ 164.508) and the Common Rule's requirements for informed consent (Common Rule, § __.116) contain important differences. For example, unlike the Common Rule, the proposed rule would have required that the authorization include a description of the information to be used or disclosed that identifies the information in a specific and meaningful way, an expiration date, and where, use of disclosure of the requested information will result in financial gain to the entity, a statement that such gain will result. We believe that the authorization requirements provide individuals with information necessary to determine whether to authorize a specific use or disclosure of protected health information about themselves, that are not required by the Common Rule.

Therefore, in the final rule, we retain the requirement for authorization for all uses and disclosures of protected health information not otherwise permitted without authorization by the rule. Some of the proposed requirements for authorization were modified in the final rule as discussed in the preamble on § 164.508. The comments received on specific proposed elements of authorization as they would have pertained to research are addressed below.

Comment: A number of commenters, including several from industry and consumer groups, recommended that the final rule require patients' informed consent as stipulated in the Common Rule. These commenters asserted that the proposed authorization document was inadequate for research uses and disclosures of protected health information since it included fewer elements than required for informed consent under the Common Rule, including for example, the Common Rule's requirement that the informed consent document include: (1) A description of any reasonably foreseeable risks or discomforts to the subject; (2) a description of any benefits to the subject or to others which may reasonably be expected from the research (Common Rule, § __.116(a)).

Response: While we agree that the ethical conduct of research requires the voluntary informed consent of research subjects, as stipulated in the Common Rule, as we have stated elsewhere, the privacy rule is limited to protecting the confidentiality of individually identifiable health information, and not protecting human subjects more broadly. Therefore, we believe it would not be within the scope of the final rule to require informed consent as stipulated by the Common Rule for research uses and disclosures of protected health information.

Comment: Several commenters specifically objected to the authorization requirement for a ''expiration date.'' To remedy this concern, many of these commenters proposed that the rule exempt research from the requirement for an expiration date if an IRB has reviewed and approved the research study. In particular, some commenters asserted that the requirement for an expiration date would be impracticable in the context of clinical trials, where the duration of the study depends on several different factors that cannot be predicted in advance. These commenters argued that determining an exact date would be impossible due to the legal requirements that manufactures and the Food and Drug Administration be able to retrospectively audit the source documents when patient data are used in clinical trials. In addition, some commenters asserted that a requirement for an expiration date would force researchers to designate specific expiration dates so far into the future as to render them meaningless.

Response: We agree with commenters that an expiration date is not always possible or meaningful. In the final rule, we continue to require an identifiable expiration, but permit it to be a specific date or an event directly relevant to the individual or the purpose of the authorization *(e.g.,* for the duration of a specific research study) in which the individual is a participant.

Comment: A number of commenters, including those from the pharmaceutical industry, were concerned about the authorization requirement that gave patients the right to revoke consent for participation in clinical research. These commenters argued that such a right to revoke authorization for the use of their protected health information would require complete elimination of the information from the record. Some stated that in the conduct of clinical trials, the retrieval of individually identifiable health information that has already been blinded and anonymized, is not only burdensome, but should this become a widespread practice, would render the trial invalid. One commenter suggested that the Secretary modify the proposed regulation to allow IRBs or privacy boards to determine the duration of authorizations and the circumstances under which a research participant should be permitted to retroactively revoke his or her authorization to use data already collected by the researcher.

Response: We agree with these concerns. In the final rule we have clarified that an individual cannot revoke an authorization to the extent that action has been taken in reliance on the authorization. Therefore, if a covered entity has already used or disclosed protected health information for a research study pursuant to an authorization obtained as required by § 164.508, the covered entity is not required under the rule, unless it agreed otherwise, to destroy protected health information that was collected, nor retrieve protected health information that was disclosed under such an authorization. However, once an individual has revoked an authorization, no additional protected health information may be used or disclosed unless otherwise permitted by this rule.

Comment: Some commenters were concerned that the authorization requirement to disclose ''financial gain'' would be problematic as it would pertain to research. These commenters asserted that this requirement could mislead patients and would make it more difficult to attract volunteers to participate in research. One commenter recommended that the statement be revised to state ''that the clinical investigator will be compensated for the value of his/her services in administrating this clinical trial.'' Another commenter recommended that the authorization requirement for disclosure of financial gain be defined in accordance with FDA's financial disclosure rules.

Response: We strongly believe that a requirement for the disclosure of financial gain is imperative to ensure that individuals are informed about how and why protected health information about themselves will be used or disclosed. We agree, however, that the language of the proposed requirement could cause confusion, because most activities involve some type of financial gain. Therefore, in the final rule, we have modified the language to provide that when the covered entity initiates

the authorization and the covered entity will receive direct or indirect remuneration (rather than financial gain) from a third party in exchange for using or disclosing the health information, the authorization must include a statement that such remuneration will result.

Comment: A few commenters asserted that the requirement to include a statement in which the patient acknowledged that information used or disclosed to any entity other than a health plan or health care provider may no longer be protected by federal privacy law would be inconsistent with existing protections implemented by IRBs under the Common Rule. In particular they stated that this inconsistency exists because IRBs are required to consider the protections in place to protect patients' confidential information and that IRBs are charged with ensuring that researchers comply with the confidentiality provisions of the informed consent document.

Response: We disagree that this proposed requirement would pose a conflict with the Common Rule since the requirement was for a statement that the ''information may no longer be protected by the federal privacy law.'' This statement does not pertain to the protections provided under the Common Rule. In addition, while we anticipate that IRBs and privacy boards will most often waive all or none of the authorization requirements, we clarify an IRB or privacy board could alter this requirement, among others, if the documentation requirements of § 164.512(i) have been met.

Reviews Preparatory to Research

Comment: Some industry groups expressed concern that the research provision would prohibit physicians from using patient information to recruit subjects into clinical trials. These commenters recommended that researchers continue to have access to hospitals' and clinics' patient information in order to recruit patients for studies.

Response: Under the proposed rule, even if the researcher only viewed the medical record at the site of the covered entity and did not record the protected health information in a manner that patients could be identified, such an activity would have constituted a use or disclosure that would have been subject to proposed § 164.508 or proposed § 164.510. Based on the comments received and the fact finding we conducted with the research community, we concluded that documentation of IRB or privacy board approval could halt the development of research hypotheses that require access to protected health information before a formal protocol can be developed and brought to an IRB or privacy board for approval. To avoid this unintended result, the final rule permits covered health care providers and health plans to use or disclose protected health information for research if the covered entity obtains from the researcher representations that: (1) 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; (2) no protected health information is to be removed from the covered entity by the researcher in the course of the review; and (3) the protected health information for which use or access is sought is necessary for the research purposes.

Comment: A few commenters asserted that the final rule should eliminate the possibility that research requiring access to protected health information could be determined to be ''exempt'' from IRB review, as provided by the Common Rule (§ __.101(b)(4)).

Response: The rule did not propose nor intend to modify any aspect of the Common Rule, including the provision that exempts from coverage, ''research involving the collection or study of existing data, documents, records, pathological specimens, or diagnostic specimens, if these sources are publically available, or if the information is recorded by the investigator in such a manner that subjects cannot be identified, directly or indirectly through identifiers linked to the subjects' (§ __.101(b)(4)). For the reasons discussed above, we have included a provision in the final rule for reviews preparatory to research that was modeled on this exemption to the Common Rule.

Deceased Persons Exception for Research

Comment: A few commenters expressed support for the proposal to allow use and disclosure of protected health information about decedents for research purposes without the protections afforded to the protected health information of living individuals. One commenter, for example, explained that it extensively uses such information in its research, and any restrictions were likely to impede its efforts. Alternately, a number of commenters provided arguments for eliminating the research exception for deceased persons. They commented that the same concerns regarding use and disclosure of genetic and hereditary information for other purposes apply in the research context. They believed that in many cases the risk of identification was greater in the research context because researchers may attempt to identify genetic and hereditary conditions of the deceased. Finally, they argued that while information of the deceased does not necessarily identify living relatives by name, living relatives could be identified and suffer the same harm as if their own medical records were used or disclosed for research purposes. Another commenter stated that the exception was unnecessary, and that existing research could and should proceed under the requirements in proposed § 164.510 that dictated the IRB/privacy board approval process or be conducted using de-identified information. This commenter further stated that in this way, at least there would be some degree of assurance that all reasonable steps are taken to protect deceased persons' and their families' confidentiality.

Response: Although we understand the concerns raised by commenters, we believe those concerns are outweighed by the need to keep the research-related policies in this rule as consistent as possible with standard research practice under the Common Rule, which does not consider deceased persons to be ''human subjects.'' Thus, we retain the exception in the final rule. With regard to the protected health information about a deceased individual, therefore, a covered entity is permitted to use or disclose such information for research purposes without obtaining authorization from a personal representative and absent approval by an IRB or privacy board as governed by § 164.512(i). We note that the National Bioethics Advisory Committee (NBAC) is currently considering revising the Common Rule's definition of ''human subject'' with regard to coverage of the deceased. However, at this time, NBAC's deliberations on this issue are not yet completed and any reliance on such discussions would be premature.

The final rule requires at § 164.512(i)(1)(iii) that covered entities obtain from the researcher (1) representation that the use or disclosure is sought solely for research on the protected health information of decedents; (2) documentation, at the request of the covered entity, of the death of such individuals; and (3) representation that the protected health information for which use or disclosure is sought is necessary for the research purposes. It is our intention with this change to reduce the burden and ambiguity on the part of the covered entity to determine whether or not the

request is for protected health information of a deceased individual.

Comment: Some commenters, in their support of the research exception, requested that HHS clarify in the final rule that protected health information obtained during the donation process of eyes and eye tissue could continue to be used or disclosed to or by eye banks for research purposes without an authorization and without IRB approval. They expressed concern over the impediments to this type of research these approvals would impose, such as added administrative burden and vulnerabilities to the time sensitive nature of the process.

Another commenter similarly expressed the position that, with regard to uses and disclosures of protected health information for tissue, fluid, or organ donation, the regulation should not present an obstacle to the transfer of donations unsuitable for transplant to the research community. However, they believed that consent can be obtained for such purposes since the donor or donor's family must generally consent to any transplant purposes, it would seem to be a minimal additional obligation to seek consent for research purposes at the same time, should the material be unsuitable for transplant.

Response: Protected health information about a deceased individual, including information related to eyes and eye tissue, can be used or disclosed further for research purposes by a covered entity in accordance with § 164.512(i)(1)(iii) without authorization or IRB or privacy board approval. This rule does not address whether organs unsuitable for transplant may be transferred to researchers with or without consent.

Modification of the Common Rule

Comment: We received a number of comments that interpreted the proposed rule as having unnecessarily and inappropriately amended the Common Rule. Assuming that the Common Rule was being modified, these comments argued that the rule was legally deficient under the Administrative Procedures Act, the Regulatory Flexibility Act, and other controlling Executive orders or laws.

In addition, one research organization expressed concern that, by involving IRBs in the process of approving a waiver of authorization for disclosure purposes and establishing new criteria for such waiver approvals, the proposed rule would have subjected covered entities whose IRBs failed to comply with the requirements for reviewing and approving research to potential sanctions under HIPAA. The comment recommended that the rule be changed to eliminate such a punitive result. Specifically, the comment recommended that the existing Common Rule structure be preserved for IRB-approved research, and that the waiver of authorization criteria for privacy purposes be kept separate from the other functions of the IRB.

Response: We disagree with the comments asserting the proposed rule attempted to change the Common Rule. It was not our intent to modify or amend the Common Rule or to regulate the activities of the IRBs with respect to the underlying research. We therefore reject the comments about legal deficiencies in the rule which are based on the mistaken perception that the Common Rule was being amended. The proposed rule established new requirements for covered entities before they could use or disclose protected health information for research without authorization. The proposed rule provided that one method by which a covered entity could obtain the necessary documentation was to receive it from an IRB. We did not mandate IRBs to perform such reviews, and we expressly provided for means other than through IRBs for covered entities to obtain the required documentation.

In the final rule, we also have clarified our intent not to interfere with existing requirements for IRBs by amending the language in the waiver criteria to make clear that these criteria relate to the privacy interests of the individual and are separate from the criteria that would be applied by an IRB to any evaluation of the underlying research. Moreover, we have restructured the final rule to also make clear that we are regulating only the content and conditions of the documentation upon which a covered entity may rely in making a disclosure of protected health information for research purposes.

We cannot and do not purport to regulate IRBs or modify the Common Rule through this regulation. We cannot under this rule penalize an IRB for failure to comply with the Common Rule, nor can we sanction an IRB based on the documentation requirements in the rule. Health plans and covered health care providers may rely on documentation from an IRB or privacy board concerning the alteration or waiver of authorization for the disclosure of protected health information for research purposes, provided the documentation, on its face, meets the requirements in the rule. Health plans and covered health care providers will not be penalized for relying on facially adequate documentation from an IRB. Health plans and covered health providers will only be penalized for their own errors or omissions in following the requirements of the rule, and not those of the IRB.

Use Versus Disclosure

Comment: Many of the comments supported the proposed rule's provision that would have imposed the same requirements for both research uses and research disclosures of protected health information.

Response: We agree with these comments. In the final rule we retain identical use and disclosure requirements for research uses and disclosures of protected health information by covered entities.

Comment: In contrast, a few commenters recommended that there be fewer requirements on covered entities for internal research uses of protected health information.

Response: For the reasons discussed above in § 164.501 on the definition of ''research,'' we disagree that an individual's privacy interest is of less concern when covered entities use protected health information for research purposes than when covered entities disclose protected health information for research purposes. Therefore, in the final rule, the research-related requirements of § 164.512(i) apply to both uses and disclosures of protected health information for research purposes without authorization.

Additional Resources for IRBs

Comment: A few commenters recommended that HHS work to provide additional resources to IRBs to assist them in meeting their new responsibilities.

Response: This recommendation is beyond our statutory authority under HIPAA, and therefore, cannot be addressed by the final rule. However, we fully agree that steps should be taken to moderate the workload of IRBs and to ensure adequate resources for their activities. Through the Office for Human Research Protections, the Department is committed to working with institutions and IRBs to identify efficient ways to optimize utilization of resources, and is committed to developing guidelines for appropriate staffing and workload levels for IRBs.

Additional Suggested Requirements

Comment: One commenter recommended that the documentation of IRB or privacy board approval also be required to state that, ''the health researcher has fully disclosed which of

the protected health information to be collected or created would be linked to other protected health information, and that appropriate safeguards be employed to protect information against re-identification or subsequent unauthorized linkages.''

Response: The proposed provision for the use or disclosure of protected health information for research purposes without authorization only pertained to individually identifiable health information. Therefore, since the information to be obtained would be individually identifiable, we concluded that it was illogical to require IRBs and privacy boards document that the researcher had ''fully disclosed that * * * appropriate safeguards be employed to protect information against re-identification or subsequent unauthorized linkages.'' Therefore, we did not incorporate this recommendation into the final rule.

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

Comment: Several commenters generally stated support for proposed § 164.510(k), which was titled ''Uses and Disclosures in Emergency Circumstances.'' One commenter said that ''narrow exceptions to confidentiality should be permitted for emergency situations such as duty to warn, duty to protect, and urgent law enforcement needs.'' Another commented that the standard '' * * * based on a reasonable belief that the disclosures are necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual'' would apply in only narrow treatment circumstances. Some commenters suggested that the provision be further narrowed, for example, with language specifically identifying ''imminent threats'' and a ''chain-of-command clearance process,'' or by limiting permissible disclosures under this provision to ''public health emergencies,'' or ''national emergencies.'' Others proposed procedural requirements, such as specifying that such determinations may only be made by the patient's treating physician, a licensed mental health care professional, or as validated by three physicians. One commenter recommended stating that the rule is not intended to create a duty to warn or to disclose protected health information but rather permits such disclosure in emergency circumstances, consistent with other applicable legal or ethical standards.

Response: We agree with the commenters who noted that the proposed provision would apply in rare circumstances. We clarify, however, that we did not intend for the proposed provision to apply to emergency treatment scenarios as discussed below. In the final rule, to avoid confusion over the circumstances in which we intend this section to apply, we retitle it ''Uses and Disclosures to Avert a Serious Threat to Health or Safety.''

We do not believe it would be appropriate to narrow further the scope of permissible disclosures under this section to respond to specifically identified ''imminent threats,'' a ''public health emergency,'' or a ''national emergency.'' We believe it would be impossible to enumerate all of the scenarios that may warrant disclosure of protected health information pursuant to this section. Such cases may involve a small number of people and may not necessarily involve a public health emergency or a national emergency.

Furthermore, in response to comments arguing that the proposed provision was too broad, we note that under both the NPRM and the final rule, we allow but do not require disclosures in situations involving serious and imminent threats to health or safety. Health plans and covered health care providers may make the disclosures allowed under § 164.512(j) consistent with applicable law and standards of ethical conduct.

As indicated in the preamble to the NPRM, the proposed approach is consistent with statutory and case law addressing this issue. The most well-known case on the topic is Tarasoff v. Regents of the University of California, 17 Cal. 3d 425 (1976), which established a duty to warn those at risk of harm when a therapist's patient made credible threats against the physical safety of a specific person. The Supreme Court of California found that the therapist involved in the case had an obligation to use reasonable care to protect the intended victim of his patient against danger, including warning the victim of the peril. Many states have adopted, in statute or through case law, versions of the Tarasoff duty to warn or protect. Although Tarasoff involved a psychiatrist, this provision is not limited to disclosures by psychiatrists or other mental health professionals. As stated in the preamble of the NPRM, we clarify that § 164.512(j) is not intended to create a duty to warn or disclose protected health information.

Comment: Several comments addressed the portion of proposed § 164.510(k) that would have provided a presumption of reasonable belief to covered entities that disclosed protected health information pursuant to this provision, when such disclosures were made in good faith, based on credible representation by a person with apparent knowledge or authority. Some commenters recommended that this standard be applied to all permissible disclosures without consent or to such disclosures to law enforcement officials.

Alternatively, a group representing health care provider management firms believed that the proposed presumption of reasonable belief would not have provided covered entities with sufficient protection from liability exposure associated with improper uses or disclosures. This commenter recommended that a general good-faith standard apply to covered entities' decisions to disclose protected health information to law enforcement officials. A health plan said that HHS should consider applying the standard of reasonable belief to all uses and disclosures that would have been allowed under proposed § 164.510. Another commenter questioned how the good-faith presumption would apply if the information came from a confidential informant or from a person rather than a doctor, law enforcement official, or government official. (The NPRM listed doctors, law enforcement officials, and other government officials as examples of persons who may make credible representations pursuant to this section.)

Response: As discussed above, this provision is intended to apply in rare circumstances—circumstances that occur much less frequently than those described in other parts of the rule. Due to the importance of averting serious and imminent threats to health and safety, we believe it is appropriate to apply a presumption of good faith to covered entities disclosing protected health information under this section. We believe that the extremely time-sensitive and urgent conditions surrounding the need to avert a serious and imminent threat to the health or safety are fundamentally different from those involved in disclosures that may be made pursuant to other sections of the rule. Therefore, we do not believe it would be appropriate to apply to other sections of the rule the presumption of good faith that applies in § 164.512(j). We clarify that we intend for the presumption of good faith to apply if the disclosure is made in good faith based upon a credible representation by any person with apparent knowledge or authority—not just by doctors, law enforcement or other government officials. Our listing of these persons in the NPRM was illustrative only, and it was not intended to limit the types of

persons who could make such a credible representation to a covered entity.

Comment: One commenter questioned under what circumstances proposed § 164.510(k) would apply instead of proposed § 164.510(f)(5), ''Urgent Circumstances,'' which permitted covered entities to disclose protected health information to law enforcement officials about individuals who are or are suspected to be victims of a crime, abuse, or other harm, if the law enforcement official represents that the information is needed to determine whether a violation of law by a person other than the victim has occurred and immediate law enforcement activity that depends upon obtaining such information may be necessary.

Response: First, we note that inclusion of this provision as § 164.510(f)(5) was a drafting error which subsequently was clarified in technical corrections to the NPRM. In fact, proposed § 164.510(f)(3) addressed the identical circumstances, which in this subsection were titled ''Information about a Victim of Crime or Abuse.'' The scenarios described under § 164.510(f)(3) may or may not involve serious and imminent threats to health or safety.

Second, as discussed in the main section of the preamble to § 164.512(j), we recognize that in some situations, more than one section of this rule potentially could apply with respect to a covered entity's potential disclosure of protected health information. We clarify that if a situation fits one section of the rule (*e.g.,* § 164.512(j) on serious and imminent threats to health or safety), health plans and covered health care providers 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)(2) or 164.512(f)(3), regarding disclosure of protected health information about suspects or victims to law enforcement officials), except as otherwise stated in the rule.

Comment: A state health department indicated that the disclosures permitted under this section may be seen as conflicting with existing law in many states.

Response: As indicated in the regulation text for § 164.512(j), this section allows disclosure consistent with applicable law and standards of ethical conduct. We do not preempt any state law that would prohibit disclosure of protected health information in the circumstances to which this section applies. (See Part 160, Subpart B.)

Comment: Many commenters stated that the rule should require that any disclosures should not modify ''duty to warn'' case law or statutes.

Response: The rule does not affect case law or statutes regarding ''duty to warn.'' In § 164.512(j), we specifically permit covered entities to disclose protected health information without authorization for the purpose of protecting individuals from imminent threats to health and safety, consistent with state laws and ethical obligations.

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

Military Purposes

Armed Forces Personnel and Veterans

Comment: A few comments opposed the proposed rule's provisions on the military, believing that they were too broad. Although acknowledging that the Armed Forces may have legitimate needs for access to protected health data, the commenters believed that the rule failed to provide adequate procedural protections to individuals. A few comments said that, except in limited circumstances or emergencies, covered entities should be required to obtain authorization before using or disclosing protected health information. A few comments also expressed concern over the proposed rule's lack of specific safeguards to protect the health information of victims of domestic violence and abuse. While the commenters said they understood why the military needed access to health information, they did not believe the rule would impede such access by providing safeguards for victims of domestic violence or abuse.

Response: We note that the military comprises a unique society and that members of the Armed Forces do not have the same freedoms as do civilians. The Supreme Court held in *Goldman* v. *Weinberger,* 475 US 503 (1986), that the military must be able to command its members to sacrifice a great many freedoms enjoyed by civilians and to endure certain limits on the freedoms they do enjoy. The Supreme Court also held in *Parker* v. *Levy,* 417 US 733 (1974), that the different character of the military community and its mission required a different application of Constitutional protections. What is permissible in the civilian world may be impermissible in the military. We also note that individuals entering military service are aware that they will not have, and enjoy, the same rights as others.

The proposed rule would have authorized covered entities to use and disclose protected health information about armed forces personnel only for activities considered necessary by appropriate military command authorities to assure the proper execution of the military mission. In order for the military mission to be achieved and maintained, military command authorities need protected health information to make determinations regarding individuals' medical fitness to perform assigned military duties.

The proposed rule required the Department of Defense (DoD) to publish a notice in the **Federal Register** identifying its intended uses and disclosures of protected health information, and we have retained this approach in the final rule. This notice will serve to limit command authorities' access to protected health information to circumstances in which disclosure of protected health information is necessary to assure proper execution of the military mission.

With respect to comments regarding the lack of procedural safeguards for individuals, including those who are victims of domestic violence and abuse, we note that the rule does not provide new authority for covered entities providing health care to individuals who are Armed Forces personnel to use and disclose protected health information. Rather, the rule allows the Armed Forces to use and disclose such information only for those military mission purposes which will be published separately in the **Federal Register**. In addition, we note that the Privacy Act of 1974, as implemented by the DoD, provides numerous protections to individuals.

We modify the proposal to publish privacy rules for the military in the **Federal Register**. The NPRM would have required this notice to include information on the activities for which use or disclosure of protected health information would occur in order to assure proper execution of the military mission. We believe that this proposed portion of the notice is redundant and thus unnecessary in light the rule's application to military services. In the final rule, we eliminate this proposed section of the notice, and we state that health plans and covered health care providers may use and disclose protected health information of Armed Forces personnel for activities considered necessary by appropriate military command authorities to assure the proper execution of a military mission, where the appropriate military authority has published a **Federal Register** notice identifying: (1) The appropriate military command authorities; and (2) the purposes for

which protected health information may be used or disclosed.

Comment: A few commenters, members of the affected beneficiary class, which numbers approximately 2.6 million (active duty and reserve military personnel), opposed proposed § 164.510(m) because it would have allowed a non-governmental covered entity to provide protected health information without authorization to the military. These commenters were concerned that military officials could use the information as the basis for taking action against individuals.

Response: The Secretary does not have the authority under HIPAA to regulate the military's re-use or re-disclosure of protected health information obtained from health plans and covered health care providers. This provision's primary intent is to ensure that proper military command authorities can obtain needed medical information held by covered entities so that they can make appropriate determinations regarding the individual's medical fitness or suitability for military service. Determination that an individual is not medically qualified for military service would lead to his or her discharge from or rejection for service in the military. Such actions are necessary in order for the Armed Forces to have medically qualified personnel, ready to perform assigned duties. Medically unqualified personnel not only jeopardize the possible success of a mission, but also pose an unacceptable risk or danger to others. We have allowed such uses and disclosures for military activities because it is in the Nation's interest.

Separation or Discharge from Military Service

Comment: The preamble to the NPRM solicited comments on the proposal to permit the DoD to transfer, without authorization, a service member's military medical record to the Department of Veterans Affairs (DVA) when the individual completed his or her term of military service. A few commenters opposed the proposal, believing that authorization should be obtained. Both the DoD and the DVA supported the proposal, noting that transfer allows the DVA to make timely determinations as to whether a veteran is eligible for benefits under programs administered by the DVA.

Response: We note that the transfer program was established based on recommendations by Congress, veterans groups, and veterans; that it has existed for many years; and that there has been no objection to, or problems associated with, the program. We also note that the Department of Transportation (DoT) and the Department of Veterans Affairs operate an analogous transfer program with respect to United States Coast Guard personnel, who comprise part of the U.S. Armed Forces. The protected health information involved the DoD/DVA transfer program is being disclosed and used for a limited purpose that directly benefits the individual. This information is covered by, and thus subject to the protections of, the Privacy Act. For these reasons, the final rule retains the DoD/DVA transfer program proposed in the NPRM. In addition, we expand the NPRM's proposed provisions regarding the Department of Veterans Affairs to include the DoT/DVA program, to authorize the continued transfer of these records.

Comment: The Department of Veterans Affairs supported the NPRM's proposal to allow it to use and disclose protected health information among components of the Department so that it could make determinations on whether an individual was entitled to benefits under laws administered by the Department. Some commenters said that the permissible disclosure pursuant to this section appeared to be sufficiently narrow in scope, to respond to an apparent need. Some commenters also said that the DVA's ability to make benefit determinations would be hampered if an individual declined to authorize release of his or her protected health information. A few commenters, however, questioned whether such an exchange of information currently occurs between the components. A few commenters also believed the proposed rule should be expanded to permit sharing of information with other agencies that administer benefit programs.

Response: The final rule retains the NPRM's approach regarding use and disclosure of protected health information without authorization among components of the DVA for the purpose of making eligibility determinations based on commenters' assessment that the provision was narrow in scope and that an alternative approach could negatively affect benefit determinations for veterans. We modify the NPRM language slightly, to clarify that it refers to a health plan or covered health care provider that is a component of the DVA. These component entities may use or disclose protected health information without authorization among various components of the Department to determine eligibility for or entitlement to veterans' benefits. The final rule does not expand the scope of permissible disclosures under this provision to allow the DVA to share such information with other agencies. Other agencies may obtain this information only with authorization, subject to the requirements of § 164.508.

Foreign Military Personnel

Comments: A few comments opposed the exclusion of foreign diplomatic and military personnel from coverage under the rule. These commenters said that the mechanisms that would be necessary to identify these personnel for the purpose of exempting them from the rule's standards would create significant administrative difficulties. In addition, they believed that this provision would have prohibited covered entities from making disclosures allowed under the rule. Some commenters were concerned that implementation of the proposed provision would result in disparate treatment of foreign military and diplomatic personnel with regard to other laws, and that it would allow exploitation of these individuals' health information. These commenters believed that the proposed rule's exclusion of foreign military and diplomatic personnel was unnecessarily broad and that it should be narrowed to meet a perceived need. Finally, they noted that the proposed exclusion could be affected by the European Union's Data Protection Directive.

Response: We agree with the commenters' statement that the NPRM's exclusion of foreign military and diplomatic personnel from the rule's provisions was overly broad. Thus, the final rule's protections apply to these personnel. The rule covers foreign military personnel under the same provisions that apply to all other members of the U.S. Armed Forces, as described above. Foreign military authorities need access to protected health information for the same reason as must United States military authorities: to ensure that members of the armed services are medically qualified to perform their assigned duties. Under the final rule, foreign diplomatic personnel have the same protections as other individuals.

Intelligence Community

Comments: A few commenters opposed the NPRM's provisions regarding protected health information of intelligence community employees and their dependents being considered for postings overseas, on the grounds that the scope of permissible disclosure without authorization was too broad. While acknowledging that the intelligence community may have legitimate needs for its employees' protected health information, the commenters believed that the NPRM

failed to provide adequate procedural protections for the employees' information. A few comments also said that the intelligence community should be able to obtain their employees' health information only with authorization. In addition, commenters said that the intelligence community should make disclosure of protected health information a condition of employment.

Response: Again, we agree that the NPRM's provision allowing disclosure of the protected health information of intelligence community employees without authorization was overly broad. Thus we eliminate it in the final rule. The intelligence community can obtain this information with authorization (pursuant to § 164.508), for example, when employees or their family members are being considered for an oversees assignment and when individuals are applying for employment with or seeking a contract from an intelligence community agency.

National Security and Intelligence Activities and Protective Services for the President and Others

Comment: A number of comments opposed the proposed ''intelligence and national security activities'' provision of the law enforcement section (§ 164.510(f)(4)), suggesting that it was overly broad. These commenters were concerned that the provision lacked sufficient procedural safeguards to prevent abuse of protected health information. The Central Intelligence Agency (CIA) and the Department of Defense (DoD) also expressed concern over the provision's scope. The agencies said that if implemented as written, the provision would have failed to accomplish fully its intended purpose of allowing the disclosure of protected health information to officials carrying out intelligence and national security activities other than law enforcement activities. The CIA and DoD believed that the provision should be moved to another section of the rule, possibly to proposed § 164.510(m) on specialized classes, so that authorized intelligence and national security officials could obtain individuals' protected health information without authorization when lawfully engaged in intelligence and national security activities.

Response: In the final rule, we clarify that this provision does not provide new authority for intelligence and national security officials to acquire health information that they otherwise would not be able to obtain. Furthermore, the rule does not confer new authority for intelligence, national security, or Presidential protective service activities. Rather, the activities permissible under this section are limited to those authorized under current law and regulation (e.g., for intelligence activities, 50 U.S.C. 401, *et seq.*, Executive Order 12333, and agency implementing regulatory authorities). For example, the provision regarding national security activities pertains only to foreign persons that are the subjects of legitimate and lawful intelligence, counterintelligence, or other national security activities. In addition, the provision regarding protective services pertains only to those persons who are the subjects of legitimate investigations for threatening or otherwise exhibiting an inappropriate direction of interest toward U.S. Secret Service protectees pursuant to 18 U.S.C. 871, 879, and 3056. Finally, the rule leaves intact the existing State Department regulations that strictly limit the disclosure of health information pertaining to employees (e.g., Privacy Issuances at State-24 Medical Records).

We believe that because intelligence/national security activities and Presidential/other protective service activities are discrete functions serving different purposes, they should be treated consistently but separately under the rule. For example, medical information is used as a complement to other investigative data that are pertinent to conducting comprehensive threat assessment and risk prevention activities pursuant to 18 U.S.C. 3056. In addition, information on the health of world leaders is important for the provision of protective services and other functions. Thus, § 164.512(k) of the final rule includes separate subsections for national security/intelligence activities and for disclosures related to protective services to the President and others.

We note that the rule does not require or compel a health plan or covered health care provider to disclose protected health information. Rather, two subsections of § 164.512(k) allow covered entities to disclose information for intelligence and national security activities and for protective services to the President and others only to authorized federal officials conducting these activities, when such officials are performing functions authorized by law.

We agree with DoD and CIA that the NPRM, by including these provisions in the law enforcement section (proposed § 164.510(f)), would have allowed covered entities to disclose protected health information for national security, intelligence, and Presidential protective activities only to law enforcement officials. We recognize that many officials authorized by law to carry out intelligence, national security, and Presidential protective functions are not law enforcement officials. Therefore, the final rule allows covered entities to disclose protected health information pursuant to this provision not only to law enforcement officials, but to all federal officials authorized by law to carry out the relevant activities. In addition, we remove this provision from the law enforcement section and include it in § 164.512(k) on uses and disclosures for specialized government functions

Medical Suitability Determinations

Comment: A few comments opposed the NPRM's provision allowing the Department of State to use protected health information for medical clearance determinations. These commenters believed that the scope of permissible disclosures under the proposed provision was too broad. While acknowledging that the Department may have legitimate needs for access to protected health data, the commenters believed that implementation of the proposed provision would not have provided adequate procedural safeguards for the affected State Department employees. A few comments said that the State Department should be able to obtain protected health information for medical clearance determinations only with authorization. A few comments also said that the Department should be able to disclose such information only when required for national security purposes. Some commenters believed that the State Department should be subject to the **Federal Register** notice requirement that the NPRM would have applied to the Department of Defense. A few comments also opposed the proposed provision on the basis that it would conflict with the Rehabilitation Act of 1973 or that it appeared to represent an invitation to discriminate against individuals with mental disorders.

Response: We agree with commenters who believed that the NPRM's provision regarding the State Department's use of protected health information without authorization was unnecessarily broad. Therefore, in the final rule, we restrict significantly the scope of protected health information that the State Department may use and disclose without authorization. First, we allow health plans and covered health care providers that are a component of the State Department to use and disclose protected health information without authorization when making medical suitability determinations for security clearance purposes. For the purposes of a security investigation, these

components may disclose to authorized State Department officials whether or not the individual was determined to be medically suitable. Furthermore, we note that the rule does not confer authority on the Department to disclose such information that it did not previously possess. The Department remains subject to applicable law regarding such disclosures, including the Rehabilitation Act of 1973.

The preamble to the NPRM solicited comment on whether there was a need to add national security determinations under Executive Order 10450 to the rule's provision on State Department uses and disclosures of protected health information for security determinations. While we did not receive comment on this issue, we believe that a limited addition is warranted and appropriate. Executive Orders 10450 and 12968 direct Executive branch agencies to make certain determinations regarding whether their employees' access to classified information is consistent with the national security interests of the United States. Specifically, the Executive Orders state that access to classified information shall be granted only to those individuals whose personal and professional history affirmatively indicates, *inter alia,* strength of character, trustworthiness, reliability, and sound judgment. In reviewing the personal history of an individual, Executive branch agencies may investigate and consider any matter, including a mental health issue or other medical condition, that relates directly to any of the enumerated factors.

In the vast majority of cases, Executive agencies require their security clearance investigators to obtain the individual's express consent in the form of a medical release, pursuant to which the agency can conduct its background investigation and obtain any necessary health information. This rule does not interfere with agencies' ability to require medical releases for purposes of security clearances under these Executive Orders.

In the case of the Department of State, however, it may be impracticable or infeasible to obtain an employee's authorization when exigent circumstances arise overseas. For example, when a Foreign Service Officer is serving at an overseas post and he or she develops a critical medical problem which may or may not require a medical evacuation or other equally severe response, the Department's medical staff have access to the employee's medical records for the purpose of making a medical suitability determination under Executive Orders 10450 and 12968. To restrict the Department's access to information at such a crucial time due to a lack of employee authorization leaves the Department no option but to suspend the employee's security clearance. This action automatically would result in an immediate forced departure from post, which negatively would affect both the Department, due to the unexpected loss of personnel, and the individual, due to the fact that a forced departure can have a long-term impact on his or her career in the Foreign Service.

For this reason, the rule contains a limited security clearance exemption for the Department of State. The exemption allows the Department's own medical staff to continue to have access to an employee's medical file for the purpose of making a medical suitability determination for security purposes. The medical staff can convey a simple ''yes'' or ''no'' response to those individuals conducting the security investigation within the Department. In this way, the Department is able to make security determinations in exigent circumstances without disclosing any specific medical information to any employees other than the medical personnel who otherwise have routine access to these same medical records in an everyday non-security context.

Second, and similarly, the final rule establishes a similar system for disclosures of protected health information necessary to determine worldwide availability or availability for mandatory service abroad under sections 101(a)(4) and 504 of the Foreign Service Act. The Act requires that Foreign Service members be suitable for posting throughout the world and for certain specific assignments. For this reason, we permit a limited exemption to serve the purposes of the statute. Again, the medical staff can convey availability determinations to State Department officials who need to know if certain Foreign Service members are available to serve at post.

Third, and finally, the final rule recognizes the special statutory obligations that the State Department has regarding family members of Foreign Service members under sections 101(b)(5) and 904 of the Foreign Service Act. 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 to determine whether a family member can accompany a Foreign Service member abroad.

Given the limited applicability of the rule, we believe it is not necessary for the State Department to publish a notice in the **Federal Register** to identify the purposes for which the information may be used or disclosed. The final rule identifies these purposes, as described above.

Correctional Institutions

Comments about the rule's application to correctional institutions are addressed in § 164.501, under the definition of ''individual.''

Section 164.512(l)—Disclosures for Workers' Compensation

Comment: Several commenters stated that workers' compensation carriers are excepted under the HIPAA definition of group health plan and therefore we have no authority to regulate them in this rule. These commenters suggested clarifying that the provisions of the proposed rule did not apply to certain types of insurance entities, such as workers' compensation carriers, and that such non-covered entities should have full access to protected health information without meeting the requirements of the rule. Other commenters argued that a complete exemption for workers' compensation carriers was inappropriate.

Response: We agree with commenters that the proposed rule did not intend to regulate workers' compensation carriers. In the final rule we have incorporated a provision that clarifies that the term ''health plan'' excludes ''any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits as defined in section 2791(c)(1) of the PHS Act.'' See discussion above under the definition of ''health plan'' in § 164.501.

Comment: Some commenters argued that the privacy rule should defer to other laws that regulate the disclosure of information to employers and workers' compensation carriers. They commented that many states have laws that require sharing of information—without consent—between providers and employers or workers' compensation carriers.

Response: We agree that the privacy rule should permit disclosures necessary for the administration of state and other workers' compensation systems. To assure that workers' compensations systems are not disrupted, we have added a new

provisions to the final rule. The new § 164.512(l) permits covered entities to disclose protected health information as authorized by and to the extent necessary to comply with workers' compensation or other similar programs established by law that provide benefits for work-related injuries or illnesses without regard to fault. We also note that where a state or other law requires a use or disclosure of protected health information under a workers' compensation or similar scheme, the disclosure would be permitted under § 164.512(a).

Comment: Several commenters stated that if workers' compensation carriers are to receive protected health information, they should only receive the minimum necessary as required in § 164.514. The commenters argued that employers and workers' compensation carriers should not have access to the entire medical history or portions of the medical history that have nothing to do with the injury in question. Further, the covered provider and not the employer or carrier should determine minimum necessary since the provider is a covered entity and only covered entities are subject to sanctions for violations of the rule. These commenters stated that the rule should clearly indicate the ability of covered entities to refuse to disclose protected health information if it went beyond the scope of the injury. Workers' compensation carriers, on the other hand, argued that permitting providers to determine the minimum necessary was inappropriate because determining eligibility for benefits is an insurance function, not a medical function. They stated that workers' compensation carriers need access to the full range of information regarding treatment for the injury underlying the claim, the claimants' current condition, and any preexisting conditions that can either mitigate the claim or aggravate the impact of the injury.

Response: Under the final rule, covered entities must comply with the minimum necessary provisions unless the disclosure is required by law. Our review of state workers' compensation laws suggests that many of these laws address the issue of the scope of information that is available to carriers and employers. The rule permits a provider to disclose information that is authorized by such a law to the extent necessary to comply with such law. Where the law is silent, the workers' compensation carrier and covered health care provider will need to discuss what information is necessary for the carrier to administer the claim, and the health care provider may disclose that information. We note that if the workers' compensation insurer has secured an authorization from the individual for the release of protected health information, the covered entity may release the protected health information described in the authorization.

Section 164.514 Requirements for Uses and Disclosures

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

General Approach

Comments: The comments on this topic almost unanimously supported the concept of de-identification and efforts to expand its use. Although a few comments suggested deleting one of the proposed methods or the other, most appeared to support the two method approach for entities with differing levels of statistical expertise.

Many of the comments argued that the standard for creation of de-identified information should be whether there is a ''reasonable basis to believe'' that the information has been de-identified. Others suggested that the ''reasonable basis'' standard was too vague.

A few commenters suggested that we consider information to be de-identified if all personal identifiers that directly reveal the identity of the individual or provide a direct means of identifying individuals have been removed, encrypted or replaced with a code. Essentially, this recommendation would require only removal of ''direct'' identifiers (e.g., name, address, and ID numbers) and allow retention of all ''indirect'' identifiers (e.g., zip code and birth date) in ''de-identified'' information. These comments did not suggest a list or further definition of what identifiers should be considered ''direct'' identifiers.

Some commenters suggested that the standard be modified to reflect a single standard that applies to all covered entities in the interest of reducing uncertainty and complexity. According to these comments, the standard for covered entities to meet for de-identification of protected health information should be generally accepted standards in the scientific and statistical community, rather than focusing on a specified list of identifiers that must be removed.

A few commenters believed that no record of information about an individual can be truly de-identified and that all such information should be treated and protected as identifiable because more and more information about individuals is being made available to the public, such as voter registration lists and motor vehicle and driver's license lists, that would enable someone to match (and identify) records that otherwise appear to be not identifiable.

Response: In the final rule, we reformulate the method for de-identification to more explicitly use the statutory standard of ''a reasonable basis to believe that the information can be used to identify the individual''—just as information is ''individually identifiable'' if there is a reasonable basis to believe that it can be used to identify the individual, it is ''de-identified'' if there is no reasonable basis to believe it can be so used. We also define more precisely how the standard should be applied.

We did not accept comments that suggested that we allow only one method of de-identifying information. We find support for both methods in the comments but find no compelling logic for how the competing interests could be met cost-effectively with only one method.

We also disagree with the comments that advocated using a standard which required removing only the direct identifiers. Although such an approach may be more convenient for covered entities, we judged that the resulting information would often remain identifiable, and its dissemination could result in significant violations of privacy. While we encourage covered entities to remove direct identifiers whenever possible as a method of enhancing privacy, we do not believe that the resulting information is sufficiently blinded as to permit its general dissemination without the protections provided by this rule.

We agree with the comments that said that records of information about individuals cannot be truly de-identified, if that means that the probability of attribution to an individual must be absolutely zero. However, the statutory standard does not allow us to take such a position, but envisions a reasonable balance between risk of identification and usefulness of the information.

We disagree with those comments that advocated releasing only truly anonymous information (which has been changed sufficiently so that it no longer represents actual information about real individuals) and those that supported using only sophisticated statistical analysis before allowing uncontrolled disclosures. Although these approaches would provide a marginally higher level of privacy protection, they would preclude many of the laudable and valuable uses discussed in the NPRM (in § 164.506(d)) and would impose too great a burden on

less sophisticated covered entities to be justified by the small decrease in an already small risk of identification.

We conclude that compared to the alternatives advanced by the comments, the approach proposed in the NPRM, as refined and modified below in response to the comments, most closely meets the intent of the statute.

Comments: A few comments complained that the proposed standards were so strict that they would expose covered entities to liability because arguably no information could ever be de-identified.

Response: In the final rule we have modified the mechanisms by which a covered entity may demonstrate that it has complied with the standard in ways that provide greater certainty. In the standard method for de-identification, we have clarified the professional standard to be used, and anticipate issuing further guidance for covered entities to use in applying the standard. In the safe harbor method, we reduced the amount of judgment that a covered entity must apply. We believe that these mechanisms for de-identification are sufficiently well-defined to protect covered entities that follow them from undue liability.

Comments: Several comments suggested that the rule prohibit any linking of de-identified data, regardless of the probability of identification.

Response: Since our methods of de-identification include consideration of how the information might be used in combination with other information, we believe that linking de-identified information does not pose a significantly increased risk of privacy violations. In addition, since our authority extends only to the regulation of individually identifiable health information, we cannot regulate de-identified information because it no longer meets the definition of individually identifiable health information. We also have no authority to regulate entities that might receive and desire to link such information yet that are not covered entities; thus such a prohibition would have little protective effect.

Comments: Several commenters suggested that we create incentives for covered entities to use de-identified information. One commenter suggested that we mandate an assessment to see if de-identified information could be used before the use or disclosure of identified information would be allowed.

Response: We believe that this final rule establishes a reasonable mechanism for the creation of de-identified information and the fact that this de-identified information can be used without having to follow the policies, procedures, and documentation required to use individually identifiable health information should provide an incentive to encourage its use where appropriate. We disagree with the comment suggesting that we require an assessment of whether de-identified information could be used for each use or disclosure. We believe that such a requirement would be too burdensome on covered entities, particularly with respect to internal uses, where entire records are often used by medical and other personnel. For disclosures, we believe that such an assessment would add little to the protection provided by the minimum necessary requirements in this final rule.

Comments: One commenter asked if de-identification was equivalent to destruction of the protected health information (as required under several of the provisions of this final rule).

Response: The process of de-identification creates a new dataset in addition to the source dataset containing the protected health information. This process does not substitute for actual destruction of the source data.

Modifications to the Proposed Standard for De-Identification

Comments: Several commenters called for clarification of proposed language in the NPRM that would have permitted a covered entity to treat information as de-identified, even if specified identifiers were retained, as long as the probability of identifying subject individuals would be very low. Commenters expressed concern that the ''very low'' standard was vague. These comments expressed concern that covered entities would not have a clear and easy way to know when information meets this part of the standard.

Response: We agree with the comments that covered entities may need additional guidance on the types of analyses that they should perform in determining when the probability of re-identification of information is very low. We note that in the final rule, we reformulate the standard somewhat to require that a person with appropriate knowledge and experience apply generally accepted statistical and scientific methods relevant to the task to make a determination that the risk of re-identification is very small. In this context, we do not view the difference between a very low probability and a very small risk to be substantive. After consulting representatives of the federal agencies that routinely de-identify and anonymize information for public release [16] we attempt here to provide some guidance for the method of de-identification.

As requested by some commenters, we include in the final rule a requirement that covered entities (not following the safe harbor approach) apply generally accepted statistical and scientific principles and methods for rendering information not individually identifiable when determining if information is de-identified. Although such guidance will change over time to keep up with technology and the current availability of public information from other sources, as a starting point the Secretary approves the use of the following as guidance to such generally accepted statistical and scientific principles and methods:

(1) Statistical Policy Working Paper 22—Report on Statistical Disclosure Limitation Methodology (*http://www.fcsm.gov/working-papers/wp22.html*) (prepared by the Subcommittee on Disclosure Limitation Methodology, Federal Committee on Statistical Methodology, Office of Management and Budget); and

(2) The Checklist on Disclosure Potential of Proposed Data Releases (*http://www.fcsm.gov/docs/checklist 799.doc*) (prepared by the Confidentiality and Data Access Committee, Federal Committee on Statistical Methodology, Office of Management and Budget).

We agree with commenters that such guidance will need to be updated over time and we will provide such guidance in the future.

According to the Statistical Policy Working Paper 22, the two main sources of disclosure risk for de-identified records about individuals are the existence of records with very unique characteristics (e.g., unusual occupation or very high salary or age) and the existence of external sources of records with matching data elements which can be used to link with the de-identified information and identify individuals (e.g., voter registration records or driver's license records). The risk of disclosure increases as the number of variables common to both types of records increases, as the accuracy or resolution of the data increases, and as the number of external sources increases. As outlined in Statistical Policy Working Paper 22, an expert disclosure analysis would also consider the probability that an individual who is the target of an attempt at re-identification is represented on both

[16] Confidentiality and Data Access Committee, Federal Committee on Statistical Methodology, Office of Management and Budget.

files, the probability that the matching variables are recorded identically on the two types of records, the probability that the target individual is unique in the population for the matching variables, and the degree of confidence that a match would correctly identify a unique person.

Statistical Policy Working Paper 22 also describes many techniques that can be used to reduce the risk of disclosure that should be considered by an expert when de-identifying health information. In addition to removing all direct identifiers, these include the obvious choices based on the above causes of the risk; namely, reducing the number of variables on which a match might be made and limiting the distribution of the records through a ''data use agreement'' or ''restricted access agreement'' in which the recipient agrees to limits on who can use/receive the data. The techniques also include more sophisticated manipulations: recoding variables into fewer categories to provide less precise detail (including rounding of continuous variables); setting top-codes and bottom-codes to limit details for extreme values; disturbing the data by adding noise by swapping certain variables between records, replacing some variables in random records with mathematically imputed values or averages across small random groups of records, or randomly deleting or duplicating a small sample of records; and replacing actual records with synthetic records that preserve certain statistical properties of the original data.

Modifications to the ''Safe Harbor''

Comments: Many commenters argued that stripping all 19 identifiers is unnecessary for purposes of de-identification. They felt that such items as zip code, city (or county), and birth date, for example, do not identify the individual and only such identifiers as name, street address, phone numbers, fax numbers, email, Social Security number, driver's license number, voter registration number, motor vehicle registration, identifiable photographs, finger prints, voice prints, web universal resource locator, and Internet protocol address number need to be removed to reasonably believe that data has been de-identified.

Other commenters felt that removing the full list of identifiers would significantly reduce the usefulness of the data. Many of these comments focused on research and, to a lesser extent, marketing and undefined ''statistical analysis.'' Commenters who represented various industries and research institutions expressed concern that they would not be able to continue current activities such as development of service provider networks, conducting ''analysis'' on behalf of the plan, studying use of medication and medical devices, community studies, marketing and strategic planning, childhood immunization initiatives, patient satisfaction surveys, and solicitation of contributions. The requirements in the NPRM to strip off zip code and date of birth were of particular concern. These commenters stated that their ability to do research and quality analysis with this data would be compromised without access to some level of information about patient age and/or geographic location.

Response: While we understand that removing the specified identifiers may reduce the usefulness of the resulting data to third parties, we remain convinced by the evidence found in the MIT study that we referred to in the preamble to the proposed rule [17] and the analyses discussed below that there remains a significant risk of identification of the subjects of health information from the inclusion of indirect identifiers such as birth date and zip code and that in many cases there will be a reasonable basis to believe that such information remains identifiable. We note that a covered entity not relying on the safe harbor may determine that information from which sufficient other identifiers have been removed but which retains birth date or zip code is not reasonably identifiable. As discussed above, such a determination must be made by a person with appropriate knowledge and expertise applying generally accepted statistical and scientific methods for rendering information not identifiable.

Although we have determined that all of the specified identifiers must be removed before a covered entity meets the safe harbor requirements, we made modifications in the final rule to the specified identifiers on the list to permit some information about age and geographic area to be retained in de-identified information.

For age, we specify that, in most cases, year of birth may be retained, which can be combined with the age of the subject to provide sufficient information about age for most uses. After considering current and evolving practices and consulting with federal experts on this topic, including members of the Confidentiality and Data Access Committee of the Federal Committee on Statistical Methodology, Office of Management and Budget, we concluded that in general, age is sufficiently broad to be allowed in de-identified information, although all dates that might be directly related to the subject of the information must be removed or aggregated to the level of year to prevent deduction of birth dates. Extreme ages—90 and over—must be aggregated further (to a category of 90+, for example) to avoid identification of very old individuals (because they are relatively rare). This reflects the minimum requirement of the current recommendations of the Bureau of the Census.[18] For research or other studies relating to young children or infants, we note that the rule would not prohibit age of an individual from being expressed as an age in months, days, or hours.

For geographic area, we specify that the initial three digits of zip codes may be retained for any three-digit zip code that contains more than 20,000 people as determined by the Bureau of the Census. As discussed more below, there are currently only 18 three-digit zip codes containing fewer than 20,000 people. We note that this number may change when information from the 2000 Decennial Census is analyzed.

In response to concerns expressed in the comments about the need for information on geographic area, we investigated the potential of allowing 5-digit zip codes or 3-digit zip codes to remain in the de-identified information. According to 1990 Census data, the populations in geographical areas delineated by 3-digit zip codes vary a great deal, from a low of 394 to a high of 3,006,997, with an average size of 282,304. There are two 3-digit zip codes containing fewer than 500 people and six 3-digit zip codes containing fewer than 10,000 people each.[19] Of the total of 881 3-digit zip codes, there are 18 with fewer than 20,000 people, 71 with fewer than 50,000 people, and 215 containing fewer than 100,000 population. We also looked at two-digit zip codes (the first 2 digits of the 5-digit zip code) and found that the smallest of the 98 2-digit zip codes contains 188,638 people.

We also investigated the practices of several other federal agencies which are mandated by Congress to release data

[17] Sweeney, L. Guaranteeing Anonymity when Sharing Medical Data, the Datafly System. Masys, D., Ed. Proceedings, American Medical Informatics Association, Nashville, TN: Hanley & Belfus, Inc., 1997:51–55.

[18] The U.S. Census Bureau's Recommendations Concerning the Census 2000 Public Use Microdata Sample (PUMS) Files [http://www.ipums.org/~census2000/2000pums bureau.pdf], Population Division, U.S. Census Bureau, November 3, 2000.

[19] Figures derived from US Census data on 1990 Decennial Census of Population and Housing, Summary Tape File 3B (STF3B). These data are available to the public (for a fee) at http://www.census.gov/mp/www/rom/msrom6af.html.