so through a business partner arrangement that meets the requirements of proposed § 164.506(e). Any services offered by the bank that are not on the list of exempt services in 1179 would be subject to the terms of this rule.

We recognize that financial institutions' role in providing information management systems to customers is evolving and that in the future, banks and credit card companies could develop and market to health plans and health care providers software designed specifically to record and track diagnostic and treatment information along with payment information. In light of the rapid evolution of information management technology available to plans and providers, we seek comment on the types of services that financial institutions are performing or may soon perform for covered entities, and how these services could be best addressed by this proposed rule.

Finally, we note that we would impose no verification requirements for most routine banking and payment activities. However, if a bank or financial institution seeks information outside payment processing transactions (e.g., during a special audit), we would require the covered entity to take reasonable steps to verify the identity of the person requesting the disclosure.

9. Uses and Disclosures for Research (§ 164.510(j))

[*Please label comments about this section with the subject: ''Research''*]

In § 164.510(j), we propose to permit covered entities to use and disclose protected health information for research without individual authorization, provided that the covered entity receives documentation that the research protocol has been reviewed by an Institutional Review Board or equivalent body—a privacy board—and that the board found that the research protocol meets specified criteria (regarding protected health information) designed to protect the subject. Absent such documentation, the subject's protected health information could be disclosed for research only with the individual's authorization, pursuant to the authorization requirements in proposed § 164.508.

Our proposed requirements for this disclosure build on the requirements for such disclosure under the Federal regulation that protects human subjects in research conducted or funded by the Federal government, the Federal Policy for the Protection of Human Subjects (often referred to as the ''Common Rule''), first published for several agencies at 56 FR 28,002–028, 032 (1991), and codified for the Department of Health and Human Services at 45 CFR part 46.

a. *Importance of research and the need for protected health information.* Much important and sometimes lifesaving knowledge has come from studies that used individually identifiable health information, including biomedical and behavioral research, epidemiological studies, health services research, and statistical activities. This type of research has lead to dramatic improvements in the nation's health. For example, the results of such research include the association of a reduction in the risk of heart disease with dietary and exercise habits, the association between the use of diethylstilbestrol (DES) by pregnant women and vaginal cancer in their daughters, and the value of beta-blocker therapy in reducing re-hospitalizations and in improving survival among elderly survivors of acute myocardial infarction.

Likewise, research on behavioral, social, and economic factors that affect health, and the effect of health on other aspects of life may require individually identifiable health information. Studies of this kind can yield important information about treatment outcomes and patterns of care, disease surveillance and trends, health care costs, risk factors for disease, functional ability, and service utilization—which may ultimately lead to improvements in the quality of patient care, the identification and eradication of public health threats, and the development of new devices and pharmaceutical products. For example, such research uncovered the fact that disease screening and treatment patterns vary with the race of the person, which in turn has lead to focused outreach programs to improve health. Such research showed that the results of certain highly invasive surgical treatments are better when the care is provided in hospitals that performed a high volume of these procedures.

It is not always possible for researchers to obtain the consent of every subject that a researcher may wish to include within a study. Thousands of records may be involved. Tracking down the subjects may entail costs that make the research impracticable. The requirement to obtain consent also may lead to biased study results, because those who refuse consent may be more or less likely than average to have a particular health problem or condition. This may be a particular concern where the research topic involves sensitive or potentially embarrassing information. At the same time, the privilege of using individually identifiable health information for research purposes without individual authorization requires that the information be used and disclosed under strict conditions that safeguard individuals' confidentiality.

b. *Definition of research.* In proposed § 164.504, we would define ''research'' as a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge. This is the definition of ''research'' in the Common Rule. This definition is well understood in the research community and elsewhere, and we propose to use it here to maintain consistency with other federal regulations that affect research.

For purposes of determining whether an activity is research under this proposed rule, it would not be relevant whether the information is given gratis, sold, bartered, rented, or otherwise provided for commercial gain. The purpose of this proposed rule regarding disclosure of protected health information for research is to protect the subjects of the information. Where the activity meets the definition of research and involves use or disclosure of protected health information, the rules in this section would apply. We request comments on any aspect of our proposed definition of research.

We understand that research and health care operations often look alike, and may overlap. We have provided definitions for these terms in § 164.504. We solicit comments on ways to further distinguish between research and operations, or otherwise clarify the application of this rule to such activities.

c. *Privacy board review requirement.* In § 154.510(j), we would require covered entities that wish to use or disclose protected health information for research without individual authorization to obtain documentation that a privacy board has reviewed the research protocol and has determined that specified criteria (described below) for waiver of authorization for use or disclosure of the information have been met. The board could be an IRB constituted under the Common Rule, or an equivalent privacy board that meets the requirements in this proposed rule. We propose to apply these requirements to uses and disclosures of protected health information by all covered entities, regardless of the source of funding of the research.

We propose no requirements for the location or sponsorship of the IRB or privacy board. The covered entity could

create such a board, and could rely on it to review proposals for uses and disclosure of records. An outside researcher could come to the covered entity with the necessary documentation from his or her own university IRB. A covered entity could engage the services of an outside IRB or privacy board to obtain the necessary documentation. The documentation would have to be reviewed by the covered entity prior to a use or disclosure subject to this provision.

Under our proposal, we would require that the documentation provided by the IRB or privacy board state: (1) That the waiver of authorization has been approved by the IRB or privacy board; (2) that the board either is an IRB established in accordance with the HHS regulations (45 CFR 46.107) or equivalent regulations of another federal agency, or is a privacy board whose members (i) have appropriate expertise for review of records research protocols, (ii) do not have a conflict of interest with respect to the research protocol, and (iii) include at least one person not affiliated with the institution conducting the research; (3) that the eight criteria for waiver of authorization (described below) are met by the protocol; and (4) the date of board approval of the waiver of authorization. We would also require that the documentation be signed by the chair of the IRB or privacy board.

i. *Application to disclosures and uses regardless of funding source.*

The Common Rule describes conditions under which research may be conducted when obtaining authorization is not possible. Those conditions are intended to ensure that research on human subjects, including research using their health records, is conducted in a manner that minimizes or eliminates the risk of harm to individuals. The Common Rule has been adopted by seventeen Federal agencies,[3] representing most of the federal agencies sponsoring human subjects research.

However, a significant amount of research involving protected health information is currently conducted in the absence of these federal protections. Pharmaceutical companies, health plans, and colleges and universities conduct research supported by private funds. Identifiable information currently is being disclosed and used by these entities without individual authorization without any assessment of risk or of whether individual privacy interests are being adequately protected.

The Secretary's Recommendations call for the extension of the Common Rule principles for waiver of authorization for research uses and disclosures of identifiable health information to all research. The Recommendations also propose additional principles that directly address waiver of authorization for research use of such information. The Recommendations would require an external board to review proposals for research on health information under criteria designed to ensure that the need for waiver of authorization is real, that the public interest in the research outweighs the individual's privacy interest, and that privacy will be protected as much as possible. In addition, the Secretary's Recommendations proposed important restrictions on use and re-disclosure of information by researchers, and requirements for safeguarding protected information, that are not currently applied under the Common Rule.

Under the Secretary's Recommendations, these requirements would apply to researchers who want to use or obtain identifiable information without first obtaining the authorization of the individual who is the subject of the information. However, under HIPAA, we do not have the authority to regulate researchers unless the researcher is also acting as a provider, as in a clinical trial. We can only directly regulate health care providers, health plans, and health care clearinghouses. This means that for most research-related disclosures of health information, we can directly regulate the entities that disclose the information, but not the recipients of the information. Therefore, in order to implement the principles in the Secretary's Recommendations, we must impose any protections on the health plans and health care providers that use and disclose the information, rather than on the researcher seeking the information.

We understand that this approach involves imposing burdens on covered entities rather than on researchers. However, our jurisdiction under this statute leaves us the choice of taking this approach, or failing to provide any protection for individuals whose information is made the subject of research, or requiring individual authorization whenever a covered entity wants to disclose protected health information for research. The second approach would provide no protection for individuals, and the third approach would make much important research impossible. Therefore, we are proposing a mechanism that we believe imposes as little burden as possible on the covered entity while providing enhanced protection for individuals. This is not the approach we advocate for new federal privacy legislation, where we would propose that standards be applied directly to researchers, but it would be a useful and appropriate approach under the HIPAA legislative authority.

We considered a number of other approaches for protecting information from research subjects, particularly when covered entities use protected health information internally for research. We considered approaches that would apply fewer requirements for internal research uses of protected health information; for example, we considered permitting covered entities to use protected health information for research without any additional review. We also considered options for a more limited review, including requiring that internal uses for research using protected health information be reviewed by a designated privacy official or by an internal privacy committee. Another option that we considered would require covered entities to have an IRB or privacy board review their administrative procedures, either for research or more generally, but not to require such review for each research project. See the preamble section II.E.9.

We are not recommending these approaches because we are concerned about applying fewer protections to subjects of private sector research than are applied to subjects of federally-funded research subject to Common Rule protections, where IRB review is required for internal research uses of protected health information. At the same time, we recognize that the proposed rule would place new requirements on research uses and disclosures for research projects not federally-funded. We solicit comment on the approach that we are proposing, including on whether the benefits of the IRB or privacy board reviews would outweigh the burdens associated with

[3] The following 17 Departments and Agencies have adopted the Common Rule: (1) Department of Agriculture; (2) Department of Commerce; (3) Department of Defense; (4) Department of Education; (5) Department of Energy; (6) Department of Health and Human Services; (7) Department of Housing and Urban Development; (8) Department of Justice; (9) Department of Transportation; (10) Department of Veterans Affairs; (11) International Development Cooperative Agency: Agency for International Development; (12) Consumer Product Safety Commission; (13) Environmental Protection Agency; (14) National Aeronautics and Space Administration; (15) National Science Foundation; (16) Social Security Administration; (17) Central Intelligence Agency. In addition, the White House Office of Science and Technology Policy is a signatory to the Common Rule, but its policy is not codified in the Code of Federal Regulations.

the proposed requirements. We also solicit comment on whether alternative approaches could adequately protect the privacy interests of research subjects. We are interested in the extent to which the proposed rule could affect the amount and quality of research undertaken by covered entities or by researchers receiving information from covered entities. People commenting on the proposed rule also may wish to address the appropriateness of applying different procedures or different levels of protection to federally and nonfederally-funded research. We would note that, as discussed below, privacy boards or IRBs could adopt procedures for ''expedited review'' similar to those provided in the Common Rule (Common Rule § ____.110) for review of records research that involves no more than minimal risk. The availability of expedited review may affect the burden associated with the proposed approach.

ii. *Documentation of privacy board approval.* We considered several options for applying Common Rule principles to research not reviewed by Common Rule IRBs through imposing requirements on covered entities. We chose the use of the privacy board because it gives covered entities the maximum flexibility consistent with protecting research subjects. Under this approach, each covered entity that wants to use or disclose protected health information for research without individual authorization could obtain the required documentation directly from an existing privacy board, an internal privacy board created by the covered entity, or from a privacy board used by the researcher.

We considered prohibiting disclosure of protected health information for research unless covered entities enter into contracts, enforceable under law, which would require the researcher to meet the review criteria. Under this approach, the covered entity would be required to enter into a contract with the researcher in order to be permitted to disclose protected health information without individual authorization. In the contract, the researcher would agree to meet the criteria described below, as well as the additional restrictions on reuse and disclosure and the physical safeguards (also described below), in exchange for obtaining the information from the covered entity.

We did not adopt this approach because of the potentially burdensome administrative costs that could stem from the need to negotiate the contracts and ensure that they are legally enforceable under law. In addition, the covered entity may have little incentive to enforce these contracts. However, we seek comments on whether the benefits of this approach outweigh the burdens, whether we could expect the burdens to be eased by the development of model contracts by local universities or professional societies, and whether covered entities could be expected to enforce these contracts. We also seek comments on whether covered entities could be given a choice between the documentation approach proposed in this NPRM and a contract approach. We are particularly interested in comments on this approach, because it appears to be the only mechanism for including restrictions on reuse and disclosure by researchers in this proposed rule.

iii. *Use of boards that are not IRBs.* The Secretary's Recommendations state that privacy protections for private sector records research should be modeled on the existing Common Rule principles. The cornerstone of the Common Rule approach to waiver of authorization is IRB approval. At the same time, we understand that Common Rule IRBs are not the only bodies capable of performing an appropriate review of records research protocols. In working with the Congress to develop comprehensive privacy legislation, we have explored the use of limited purpose privacy boards to review research involving use or disclosure of health information. If the review criteria and operating rules of the privacy board are sufficiently consistent with the principles stated in the Secretary's Recommendations to afford the same level of protection, there would be no need to insist that the review board be a formal Common Rule IRB.

Among the Common Rule requirements for IRB membership, as stated in 45 CFR 46.107, are the following:

- Each IRB must have members with varying backgrounds and appropriate professional competence as necessary to review research protocols.
- Each IRB must include at least one member who is not affiliated with the institution or related to a person who is affiliated with the institution.
- No IRB member may participate in review of any project in which the member has a conflict of interest.

We propose to require that a covered entity could not use or disclose protected health information for research without individual authorization if the board that approved the waiver of authorization does not meet these three criteria.

We considered applying the additional criteria for IRB membership stated in the Common Rule. However, many of the additional criteria are relevant to research generally, but less relevant for a board whose sole function is to review uses or disclosures of health information. In addition, the Common Rule IRB membership criteria are more detailed than the criteria for privacy board membership we propose here. Since our legislative authority reaches to covered entities, but not to the privacy board directly, we decided that imposing additional or more detailed requirements on privacy boards would impose added burdens on covered entities that did not clearly bring concomitant increases in patient protections. We continue to support more complete application of Common Rule criteria directly to these privacy boards through federal legislation. We believe the approach we propose here strikes the appropriate balancing between protecting individuals' privacy interests and keeping burdens on covered entities to a minimum.

d. *Criteria.* In § 164.510(j)(2)(iii), we propose to prohibit the use or disclosure of protected health information for research without individual authorization unless the covered entity has documentation indicating that the following criteria are met:

- The use or disclosure of protected health information involves no more than minimal risk to the subjects;
- The waiver or alteration will not adversely affect the rights and welfare of the subjects;
- The research could not practicably be carried out without the waiver or alteration;
- Whenever appropriate, the subjects will be provided with additional pertinent information after participation;
- The research would be impracticable to conduct without the protected health information;
- The research project is of sufficient importance to outweigh the intrusion into the privacy of the individual whose information would be disclosed;
- There is an adequate plan to protect the identifiers from improper use and disclosure; and
- There is an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers.

The first four criteria are in the Common Rule. (The Common Rule § ____.116(d)).[4] These criteria were

[4] It should be noted that for the Department of Defense, 10 U.S.C. 980 prohibits the waiver of informed consent. Only those studies that qualify for exemption per 45 CFR 46.101(b), or studies that do not meet the 45 CFR part 46 definition of human subjects research can be performed in the absence

Continued

designed for research generally, and not specifically to protect individuals' privacy interests regarding medical records research. For this reason, the Secretary's Recommendations include the last four criteria, which were developed specifically for research on medical records.

As part of the IRB or privacy board's review of the use of protected health information under the research protocol, we assume that in case of a clinical trial, it would also review whether any waiver of authorization could also include waiver of the subject's right of access to such information during the course of the trial. See § 164.514(b)(iv).

We recognize that the fourth criterion may create awkward situations for some researchers. Where authorization has been waived, it may be difficult to later approach individuals to give them information about the research project. However, in some cases the research could uncover information that would be important to provide to the individual (e.g., the possibility that they are ill and should seek further examination or treatment). For this reason, we are including this criterion in the proposed rule.

We also recognize that the fifth criterion, which would ask the board to weigh the importance of the research against the intrusion of privacy, would require the board to make a more subjective judgment than that required by the other criteria. This balancing, we feel, goes to the heart of the privacy interest of the individual. We understand, however, that some may view this criterion as a potential impediment to certain types of research. We solicit comment on the appropriateness of the criterion, the burden it would place on privacy boards and IRBs, and its potential effects on the ability of researchers to obtain information for research.

The Secretary's Recommendations propose that a researcher who obtains protected health information this way should be prohibited from further using or disclosing it except when necessary to lessen a serious and imminent threat to the health or safety of an individual or to the public health, or for oversight of the research project, or for a new research project approved by an IRB or similar board. In addition the Recommendations propose an obligation on researchers to destroy the identifiers unless an IRB or similar board determines that there is a research or health justification for retaining them and an adequate plan to protect them from improper disclosure.

We do not have the authority under HIPAA to place such requirements directly on researchers. While criteria to be met in advance can be certified in documentation through board review of a research protocol, a board would have no way to assess or certify a researcher's behavior after completion of the protocol (e.g., whether the researcher was engaging in improper reuse or disclosure of the information, or whether the researcher had actually destroyed identifiers). We instead propose to require the researcher to show a plan for safeguarding the information and destroying the identifiers, which the privacy board or IRB can review and evaluate in determining whether the requested disclosure is proper. We solicit comment on how to include ongoing protections for information so disclosed under this legislative authority without placing excessive burdens on covered entities.

We note that privacy boards or IRBs could adopt procedures for ''expedited review'' similar to those provided in the Common Rule (Common Rule § _____.110) Under the Common Rule's expedited review procedure, review of research that involves no more than minimal risk, and involves only individuals' medical records may be carried out by the IRB chairperson or by one or more reviewers designated by the chairperson from among the members of the IRB. The principle of expedited review could be extended to other privacy boards for disclosures for records-based research. Like expedited review under the Common Rule, a privacy board could choose to have one or more members review the proposed research.

e. *Additional provisions of this proposed rule affecting research.*

i. *Research including health care.*

To the extent that the researcher studying protected health information is also providing treatment as defined in proposed § 164.504, such as in a clinical trial, the researcher would be a covered health care provider for purposes of that treatment, and would be required to comply with all the provisions of this rule applicable to health care providers.

ii. *Individual access to research information.*

The provisions of § 164.514 of this proposed rule, regarding individual access to records, would also apply where the research includes the delivery of health care. We are proposing an exception for clinical trials where the information was obtained by a covered provider in the course of a clinical trial, the individual has agreed to the denial of access when consenting to participate in the trial (if the individual's consent to participate was obtained), and the trial is in still in progress.

iii. *Research on records of deceased persons.*

In § 164.506(f), we propose that, unlike the protections provided by the remainder of this rule, the protections of this proposed rule will end at the death of the subject for the purpose of disclosure of the subject's information for research purposes. In general, this proposed rule would apply to the protected health information of an individual for two years after the individual's death. However, requiring IRB or privacy board review of research studies that use only health information from deceased persons would be a significant change from the requirements of the Common Rule, which apply to individually identifiable information about living individuals only. In addition, some of the Common Rule criteria for waiver of authorization are not readily applicable to deceased persons. To avoid a conflict between Common Rule requirements and the requirements of this proposed rule, we are proposing that the protections of this proposed rule end at the death of the subject for the purpose of disclosure of the subject's information for research purposes.

iv. *Verification.*

In § 164.518(c), we propose to require covered entities to verify the identity of most persons making requests for protected health information and, in some cases, the legal authority behind that request. For disclosures of protected health information for research purposes under this subsection, the required documentation of IRB or privacy board approval would constitute sufficient verification. No additional verification would be necessary under § 164.518(c).

f. *Application to research covered by the Common Rule.* Some research projects would be covered by both the Common Rule and the HIPAA regulation. This proposed rule would not override the Common Rule. Thus, where both the HIPAA regulation and the Common Rule would apply to research conducted by a covered entity, both sets of regulations would need to be followed. Because only half of the substantive criteria for board approval proposed in this rule are applied by IRBs today, this would entail new responsibilities for IRBs in these situations. However, we believe that the additional burden would be minimal, since the IRBs will already be reviewing the research protocol, and will be asked

---

of a process to provide informed consent to prospective subjects. This proposed rule would not affect DOD's implementation of 10 U.S.C. 980.

only to assess the protocol against some additional criteria. This burden is justified by the enhancement of privacy protections gained by applying rules specifically designed to protect the subjects of medical records research.

We considered excluding research covered by the Common Rule from the provisions of this proposed rule. We rejected this approach for two reasons. First, the additional proposed requirements applied through HIPAA are specifically designed to protect the privacy interests of the research subjects, and the small additional burden on IRBs would be outweighed by the improved protections for individuals. Second, such an approach would allow federally-funded research to proceed under fewer restrictions than privately funded research. We believe that the source of funding of the research should not determine the level of protection afforded to the individual.

We note that the definition of ''identifiable'' information proposed in § 164.504 of this rule differs from the interpretation of the term under the Common Rule. In particular, if a covered entity encodes identifiers as required under § 164.506(d) before undertaking a disclosure of health information for research purposes, the requirements of this section would not apply. However, the encoded information would still be considered ''identifiable'' under the Common Rule and therefore may fall under the human subjects regulations.

g. *Obtaining the individual's authorization for research use or disclosure of protected health information.* If a covered entity chooses to obtain individual authorization for use or disclosure of information for research, the requirements applicable to individual authorizations for release of protected health information would apply. These protections are described in § 164.508.

For research projects to which both the Common Rule and this proposed rule would apply, both sets of requirements for obtaining the authorization of the subject for research would apply. As with criteria for waiver of authorization, this proposed rule would impose requirements for obtaining authorization that are different from Common Rule requirements for obtaining consent. In particular, the regulation would require more information to be given to individuals regarding who could see their information and how it would be used. For the reasons explained above, we are proposing that both sets of requirements apply, rather than allow federally-funded research to operate with fewer privacy protections than privately-funded research.

h. *Need to assess the Common Rule.* In general, the Common Rule was designed to protect human subjects participating in research projects from physical harm. It was not specifically designed to protect an individual's medical records when used for research. For research in which only the medical information of the human subject is used, i.e., records research, there are several ways in which the Common Rule protections could be enhanced.

In developing these proposed regulations, and in reviewing the comprehensive medical privacy legislation pending before Congress, it has become clear that the Department's human subject regulations (45 CFR part 46, 21 CFR part 50, and 21 CFR part 56) may not contain all of the safeguards necessary to protect the privacy of research participants. Because the source of research funding should not dictate the level of privacy protection afforded to a research subject, the Secretary of HHS will immediately initiate plans to review the confidentiality provisions of the Common Rule.

To further that process, we solicit comments here on how Common Rule protections for the subjects of records review should be enhanced. For example, we will consider the adequacy of the Common Rule's provisions regarding conflict of interest, expedited review, exemptions (such as the exemption for certain research on federal benefits programs), deceased subjects, and whether IRB's should place greater emphasis on confidentiality issues when reviewing research protocols. We also seek comment on whether the Common Rule requirements for obtaining consent for records research should be modified to reflect the specific risks entailed in such research.

In addition, because seventeen other Departments and Agencies are signatories to the Common Rule and each has its own human subject regulations, the Secretary of HHS will consult with these Departments and Agencies regarding potential changes to the Common Rule.

10. Uses and Disclosures in Emergency Circumstances (§ 164.510(k))

[*Please label comments about this section with the subject: ''Emergency circumstances''*]

In § 164.510 (k), we propose to permit covered entities to use or disclose protected health information in emergencies, consistent with applicable law and standards of ethical conduct, based on a reasonable belief that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of any person or the public.

a. *Importance of emergency response and the need for protected health information.* Circumstances could arise that are not otherwise covered in the rules proposed in §§ 164.510(b) and 164.510(f) for law enforcement and public health, where covered entities may need to disclose protected health information to prevent or lessen a serious and imminent threat of harm to persons or the public. Persons at risk include the individual who is the subject of the protected health information as well as others. Through their professional activities, covered entities, particularly health care providers, may obtain information that leads them to believe that an individual is at risk of harm to him or herself, or poses a threat to others. This information could be needed by emergency and first responders (including law enforcement officials) to deal with or prevent an emergency situation posing a serious and imminent threat of harm to such persons or the public.

b. *Proposed requirements.* We would permit covered entities, consistent with applicable law and standards of ethical conduct, to disclose protected health information based on a reasonable belief that the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. Covered entities would only be permitted to make such disclosures to persons who are reasonably able to prevent or lessen the threat, including to the target of the threat.

Anticipating all circumstances under which emergency disclosure could be necessary is not possible. This section must be stated in somewhat general terms. We intend to permit covered entities to respond to emergency requests for protected health information, where it is reasonable for the covered entity to believe that such disclosure would prevent or reduce a serious emergency situation. Such emergencies may threaten a single person or the general public. We do not intend to permit disclosure of protected health information in response to hypothetical scenarios or potential emergencies that are not imminent and serious. This permitted disclosure would be narrow; it should not become a loophole for disclosures not permitted by the other provisions of the proposed rule.

This provision would permit disclosure of relevant information in response to credible requests from law enforcement, public health, or other government officials. The covered entity would be permitted to reasonably rely on credible representations that an emergency exists and that protected health information could lessen the threat. If the disclosure was made in a good faith belief that these circumstances exist, it would be lawful under this section. A covered entity could also disclose protected health information on its own initiative if it determined that the disclosure were necessary, consistent with other applicable legal or ethical standards. Our proposed rule is intended to permit such disclosures where they are otherwise permitted by law or ethical standards. We do not intend to permit disclosures by health care providers or others that are currently prohibited by other law or ethical standards.

Disclosure for emergency circumstances could be authorized by statute or common law and could also be addressed in medical professional ethics and standards. For example, the American Medical Association Principles of Medical Ethics on Confidentiality provides that:

> [T]he obligation to safeguard patient confidences is subject to certain exceptions that are ethically and legally justified because of overriding social consideration. Where a patient threatens to inflict serious bodily harm to another person or to him or herself and there is a reasonable probability that the patient may carry out the threat, the physician should take reasonable precautions for the protection of the intended victim, including notification of law enforcement authorities.

The duty to warn third persons at risk has been addressed in court cases, and the provision proposed permits disclosures in accord with such legal duties. The leading case on this issue is *Tarasoff* v. *Regents of the University of California*, 17 Cal. 3d 425 (1976). In that case, 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 (judicially or legislatively) versions of the *Tarasoff* duty to warn, but not all States have done so. This proposed rule is not intended to create a duty to warn or disclose but would simply permit the disclosure under the emergency circumstances consistent with other applicable legal or ethical standards.

An emergency disclosure provision does present some risks of improper disclosure. There will be pressures and uncertainties when disclosures are requested under emergency circumstances, and decisions must often be made instantaneously and without the ability to seek individual authorization or to perform complete verification of the request. We believe that this risk would be warranted when balancing the individual's interest in confidentiality against the societal interests to preserve life and protect public safety in those rare emergency circumstances where disclosure is necessary. A covered entity that makes a reasonable judgement under such pressure and discloses protected health information in good faith would not be held liable for wrongful disclosure if circumstances later prove not to have warranted the disclosure.

We would also exempt emergency disclosures from provisions that allow individuals to request restrictions on uses and disclosures of their protected health information for treatment, payment and health care operations. In emergency situations, health care professionals need to have any information that will allow them to respond to the emergency circumstance, and cannot be expected to take the time to remind themselves of restrictions on particular information. See proposed § 164.506(c).

11. Disclosure to Next-of-Kin (§ 164.510(l))

[*Please label comments about this section with the subject: ''Next-of-kin''*]

In § 164.510(l), we propose to require health care providers to obtain a verbal agreement from the individual before disclosing protected health information to next-of-kin, to other family members, or to others with whom the individual has a close personal relationship. Where it is not practical or feasible to request and obtain such verbal agreement, providers could disclose to next-of-kin, to other family members, or to others with whom an individual has a close personal relationship, protected health information that is directly relevant to the person's involvement in the individual's care, consistent with good professional health practice and ethics.

a. *Importance of disclosures to next-of-kin and the need for protected health information.* In some cases, disclosure of protected health information to next-of-kin, to other relatives, or to persons with whom the individual has a close personal relationship and who are involved in caring for or helping the individual, can facilitate effective health care delivery. We do not intend to impede the disclosure of protected health information to relatives or friends when expeditious disclosure of such information clearly would be in the individual's best interest.

b. *Proposed requirements.* We propose that when an individual has the capacity to make his or her own health decisions, providers could disclose protected health information to the individual's next-of-kin, to other relatives, or to persons with whom the individual has a close personal relationship, if the individual has verbally agreed to such disclosure. Verbal agreement could be indicated informally, for example, from the fact that the individual brought a family member or friend to the physician appointment and is actively including the family member or friend in the discussion with the physician. If, however, the situation is less clear and the provider is not certain that the individual intends for the family member or friend to be privy to protected health information about the individual, the provider would be required to ask the individual. In these cases, when verbal agreement can be obtained, that agreement would be sufficient verification of the identity of the person to meet the requirements of § 164.518(c).

We would also permit health care providers to disclose protected health information without verbal agreement to next-of-kin, to other relatives, or to persons with whom the individual has a close personal relationship, if such agreement cannot practicably or reasonably be obtained and the disclosure is consistent with good health professional practice and ethics. When verbal agreement cannot be obtained, the provider would be required to take reasonable steps to verify the identity of the family member or friend in order to meet the verification requirement under § 164.518(c). Verbal inquiry would suffice; we would not require any specific type of identity check.

We considered requiring a written authorization for each disclosure in these situations, but rejected that option because it is not practicable and does not provide sufficient additional privacy protection to justify the burden it would place on health care providers and individuals. Many of these conversations are unscheduled and of short duration, and requiring a written authorization may impede treatment and detain the individual. Therefore we would allow a one-time verbal agreement and (where required) verification to suffice for disclosure of protected health information relevant to

the individual's care. For example, a health care provider could disclose protected health information about an individual's treatment plan to the individual's adult child who is taking the individual home from the hospital, if the provider has verbally requested and individual has agreed to providing the adult child with relevant information about aspects of the individual's health care. Disclosure also could be appropriate in cases where a verbal agreement cannot practicably be obtained. For example, a pharmacist could be guided by his or her professional judgment in dispensing a filled prescription to someone who claims to be picking it up on behalf of the individual for whom the prescription was filled.

In such cases, disclosures would have to follow the ''minimum necessary'' provisions of proposed § 164.506(b). For example, health care providers could not disclose without individual authorization extensive information about the individual's surgery or past medical history to the neighbor who is simply driving the individual home and has no need for this information. We request comment on this approach.

The proposed definition of ''individual'' addresses related disclosures regarding minors and incapacitated individuals.

12. Additional Uses and Disclosures Required by Other Law (§ 164.510(n))

[*Please label comments about this section with the subject: ''Additional uses and disclosures required by other law''*]

In § 164.510(n) we propose to allow covered entities to use or disclose protected health information if such use or disclosure is not addressed elsewhere in § 164.510, is required by other law, and the disclosure meets all the relevant requirements of such law.

Other laws may require uses or disclosures of protected health information for purposes not captured by the other provisions of proposed § 164.510. An example is State workers' compensation laws, which could require health care providers to disclose protected health information to a workers' compensation insurer or to an employer. Covered entities generally could make uses and disclosures required by such other laws.

Where such a use or disclosure would also be addressed by other provisions of this regulation, the covered entity would also have to follow the requirements of this regulation. Where the provisions of the other law requirements are contrary to the provisions in this proposed rule and more protective of the individual's privacy, the provisions of the other law would generally control. See discussion in section II.I below.

We have included this section because it is not our intention to obstruct access to information deemed important enough by other authorities to require it by law. We considered omitting this provision because we are concerned that we do not know enough about the required disclosures it would encompass, but decided to retain it in order to raise the issue of permitting disclosures for other, undetermined purposes. We solicit comment on the possible effects of omitting or narrowing this provision.

Under this section, health care providers could make reports of abuse of any person that are required by State law. All States require reports of abuse. All States require reporting to child protective agencies of instances of child abuse or neglect that they identify, and most States require similar reports of abuse or neglect of elderly persons. These are valuable requirements which we support and encourage. The Act (in section 1178(b)) specifically requires that this regulation not interfere with State requirements for reporting of abuse. Additionally, all States require health care providers to report gunshot wounds and certain other health conditions related to violence; this provision would permit such reports.

Section 164.518(c), requiring verification of the identity and legal authority of persons requesting disclosure of protected health information would apply to disclosures under § 164.510(n). As noted above, we are not familiar with all of the disclosures of protected health information that are mandated by State law, so we cannot be certain that the verification requirements in § 164.518(c) would always be appropriate. We solicit comments on whether those requirements would be appropriate for all disclosures that would be permitted here.

13. Application to Specialized Classes (§ 164.510(m))

In the following categories we propose use and disclosure provisions that respond to the unique circumstances of certain federal programs. We request comment on whether additional provisions are necessary to comply with the suitability and national security determination requirements of Executive Order 10450, as amended, and other national security laws.

a. *Application to military services.*

[*Please label comments about this section with the subject: ''Military services''*]

To address the special circumstances of the Armed Forces and their health care systems, we propose to permit military and other federal providers and health plans to use and disclose protected health information about active duty members of the Armed Forces for certain purposes, and to exclude from coverage under this rule health information about certain persons who receive care from military providers.

i. *Members of the Armed Forces.*

The primary purpose of the health care system of the military services differs in its basic character from that of the health care system of society in general. The special nature of military service is acknowledged by the Constitutional provision for separate lawmaking for them (U.S. Constitution, article I, section 8, clause 14) and in their separate criminal justice system under the Uniform Code of Military Justice (10 U.S.C. 801, *et seq.*).

The military health care system, like other federal and civilian health care systems, provides medical care and treatment to its beneficiary population. However, it also serves a critical national defense purpose, ensuring that the Armed Forces are in a state of medical readiness to permit the discharge of those responsibilities as directed by the National Command Authority.

The health and well-being of military members is key and essential. This is true whether such personnel are serving in the continental United States or overseas or whether such service is combat-related or not. In all environments, operational or otherwise, the Armed Forces must be assured that its personnel are medically qualified to perform their responsibilities. This is critical as each and every person performs a vital service upon which others must rely in executing a specified defense requirement. Unqualified personnel not only jeopardize the possible success of an assignment or operation, but they pose an undue risk and danger to others.

To assure that such persons are medically fit, health information is provided to proper command authorities regarding military members performing certain critical functions for medical screening and other purposes so that determinations can be made regarding the ability of such personnel to perform assigned duties. For example, health information is provided regarding:

- A pilot receiving medication that may affect alertness;
- An Armed Forces member with an intolerance for a vaccine necessary for deployment to certain geographical areas;
- Any significant medical or psychological changes in a military member who is a member of the Nuclear Weapons Personnel Reliability Program;
- A military recruit or member with an illness or injury which disqualifies him or her from military service;
- Compliance with controlled substances policies.

The military and the Coast Guard obtain such information from their own health care systems, as well as from other agencies that provide health care to service members, such as the Department of Transportation (DOT), which is responsible for the United States Coast Guard and other federal agencies which provide medical care to members of the Armed Forces (*e.g.*, the Department of State (DOS) provides such care to military attaches and Marine security personnel assigned to embassies and consulates overseas, the Department of Veterans Affairs provides care in certain areas of the country or in cases involving specialized services). Other health care providers could also provide information, for example, when a private sector physician treats a member injured in an accident.

The special needs of the DOD and DOT for accessing information for purposes other than treatment, payment or health care operations were recognized in the Secretary's Recommendations. We considered several options for accommodating the unique circumstances of a military health care environment. We considered providing special rule-making authority to the DOD and other federal agencies which provide care to members of the military, but HIPAA does not allow for such delegation by the Secretary of HHS. Therefore, we propose that health care providers and health plans of the DOD, the DOT, the DOS, the Department of Veterans Affairs as well as any other person or entity providing health care to Armed Forces personnel, could use or disclose protected health information without individual authorization for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission.

The appropriate military command authorities, the circumstances in which use or disclosure without individual authorization would be required, and the activities for which such use or disclosure would occur in order to assure proper execution of the military mission, would be identified through **Federal Register** notices promulgated by the DOD or the DOT (for the Coast Guard). The verification requirements in § 164.518(c) would apply to disclosures permitted without authorization.

This proposal would not confer authority on the DOD or the DOT to enact rules which would permit use or disclosure of health information that is restricted or controlled by other statutory authority.

ii. *Foreign diplomatic and military personnel.*

The Department of Defense, as well as other federal agencies, provide medical care to foreign military and diplomatic personnel, as well as their dependents. Such care is provided pursuant to either statutory authority (*e.g.*, 10 U.S.C. 2549) or international agreement. The care may be delivered either in the United States or overseas. Also, where health care is provided in the United States, it may be furnished by non-government providers when government delivered care is not available or the beneficiary elects to obtain private as opposed to government health care. Examples include:

- Foreign military personnel being trained, or assigned to U.S. military organizations, in the United States who receive care from either government or private health care providers;
- The DOD operated medical clinic which provides care to all allied military and diplomatic personnel assigned to NATO SHAPE Headquarters in Brussels, Belgium;
- The DOS, which also is engaged in arranging health care for foreign diplomatic and military personnel and their families, could also have legitimate needs for information concerning the health services involved.

We believe that the statute was not intended to cover this unique class of beneficiaries. These persons are receiving U.S., either private or governmental, furnished health care, either in the United States or overseas, because of the beneficiary's military or diplomatic status. For such personnel, we believe that the country-to-country agreements or federal statutes which call for, or authorize, such care in furtherance of a national defense or foreign policy purpose should apply. We propose to exclude foreign military and diplomatic personnel and their dependents who receive health care provided by or paid for by the DOD or other federal agency, or by an entity acting on its behalf pursuant to a country-to-country agreement or federal statute, from the definition of an ''individual'' in § 164.504. Therefore, the health information created about such persons by a DOD or other federal agency health care provider would not be protected under this rule. However, information created about such persons by covered health care providers whose services are not paid for by or provided on behalf of a federal agency would be protected health information.

iii. *Overseas foreign national beneficiaries.*

The Department of Defense, as well as other federal agencies and U.S.-based non-governmental organizations, provide health care to foreign nationals overseas incident to U.S. sponsored missions or operations. Such care is provided pursuant to federal statute, international agreement, international organization sponsorship, or incident to military operations (including humanitarian and peacekeeping operations). Examples include:

- The DOD provides general health care to an indigenous population incident to military deployment;
- The DOD provides health care to captured and detained personnel as a consequence of overseas combat operations. Such care is mandated by international agreement, i.e., the Geneva Conventions. The most recent example involves the surrender or capture of Iraqi soldiers during the conduct of Operation Desert Storm;
- A number of federal agencies and non-governmental organizations provide health care services as part of organized disaster relief or other humanitarian programs and activities around the world.

We believe that the statute did not contemplate these unique beneficiary populations. Under circumstances where healthcare is being furnished to foreign nationals incident to sanctioned U.S. activities overseas, application of these proposed rules could have the unintended effect of impeding or frustrating the conduct of such activities, and producing incongruous results. Examples include:

- Requiring preparation of a notice advising the local population of the information practices of the DOD incident to receiving free medical care as part of disaster relief.
- Medical information involving a prisoner of war could not be disclosed, without the prisoner's consent, to U.S. military authorities who have responsibility for operating the POW camps.

Therefore, we propose to exclude overseas foreign national beneficiaries of health care provided by the DOD or other federal agency, or by non-governmental organizations acting on behalf of a federal agency, from the

definition of an individual. This exclusion would mean that any health information created when providing health care to this population would not be protected health information and therefore not covered by these rules.

iv. *Disclosure to the Department of Veterans Affairs.*

Upon completion of an individual's military service, the DOD routinely transfers that person's entire military service record, including protected health information, to the Department of Veterans Affairs so the file can be retrieved quickly if the individual or his/her dependents apply for veterans benefits. This practice was initiated in an effort to expedite veterans benefits eligibility determinations by ensuring timely access to complete, accurate information on the veteran's military service. Under the proposed rule, the transfer of these files would require individual authorization if protected health information is included. While this change could increase the time necessary for benefits processing in some cases, we believe the privacy interests outweigh the related administrative challenges. We invite comment on whether our assessment of costs and benefits is accurate. We also invite comment on alternative methods for ensuring privacy while expediting benefits processing.

b. *Application to the Department of Veterans Affairs.*

[*Please label comments about this section with the subject: ''Department of Veterans Affairs''*]

We propose to permit protected health information to be used without individual authorization by and among components of the Department of Veterans Affairs that determine eligibility for or entitlement to, or that provide, benefits under laws administered by the Secretary of Veterans Affairs.

This exemption recognizes that the Veterans Administration is two separate components: The Veterans Health Administration (which operates health care facilities) and the Veterans Benefits Administration (which operates the Veterans disability program). The close integration of the operations of the two components may make requiring individual authorizations before transferring protected health information particularly disruptive. Further, the Veterans Health Administration transfers medical information on a much larger scale than most other covered entities, and requiring individual authorization for transfers among components could compromise the Department of Veterans Affairs' ability to fulfill its statutory mandates.

Nonetheless, we invite comments on this approach. In particular, we are interested in whether the requirement for individual authorization for disclosure of medical records for use in benefits calculations would increase privacy protections for veterans, or whether it would be of questionable value since most veterans would authorize disclosure if it were tied to their benefits. We also are interested in comments on whether the proposed approach would unreasonably hamper the Department of Veterans Affairs in its ability to make accurate benefits determinations in cases in which individuals chose not to authorize disclosure.

c. *Application to the Department of State.*

[*Please label comments about this section with the subject: ''Department of State''*]

We propose to permit the Department of State to use and disclose protected health information for certain purposes unrelated to its role as a health care provider but necessary for the achievement of its mission.

i. *Importance of Foreign Service determinations and the need for protected health information.*

The Secretary of State administers and directs the Foreign Service. As contemplated in the Foreign Service Act, the Foreign Service is ''to serve effectively the interests of the United States'' and ''provide the highest caliber of representation in the conduct of foreign affairs;'' members of the Foreign Service are to be available to serve in assignments throughout the world. As called for under the Foreign Service Act, the DOS has established a health care program to promote and maintain the physical and mental health of members of the Service and that of other Government employees serving abroad under chief of mission authority, as well as accompanying family members. The DOS provides health care services to thousands of Foreign Service officers, other government employees and their families serving abroad, many of whom are frequently changing posts or assignments.

Worldwide availability for service is a criterion for entrance into the Foreign Service, so that applicants with conditional offers of employment must undergo medical clearance examinations to establish their physical fitness to serve in the Foreign Service on a worldwide basis prior to entrance into the Foreign Service. Employees and accompanying family members also must be medically cleared before assignments overseas, to preclude assignment to posts where existing medical conditions would be exacerbated or where resources to support an existing medical condition are inadequate.

The DOS uses protected health information gained through its role as a health care provider to fulfill its other responsibilities. The information is used to make medical clearance and fitness decisions as well as other types of determinations requiring medical information (such as fitness for duty or eligibility for disability retirement of Foreign Service members). Such information is also used to determine whether to immediately evacuate an individual for evaluation or treatment, or to determine whether to allow an employee or family member to remain in a position or at post abroad. An individual's record can include medical information provided to the DOS with the individual's authorization by outside health care providers, protected health information about treatment provided or paid for by the DOS, and medical information collected from non-treatment processes such as the clearance process.

ii. *Proposed requirements.*

We are proposing to exempt the DOS from the requirement to obtain individual authorization (§ 164.508) in order to use or disclose protected health information maintained by its health care program in certain cases. Specifically, the exemption would apply to the disclosure or use of protected health information of the following individuals for the following purposes: (1) Of applicants to the Foreign Service for medical clearance determinations of physical fitness to serve in the Foreign Service on a worldwide basis, including: medical and mental conditions limiting assignability abroad; conformance to occupational physical standards, where applicable; and suitability;

(2) of members of the Foreign Service and other United States Government employees assigned to serve abroad under Chief of Mission authority, for (a) medical clearance determinations for assignment to posts abroad, including: medical and mental conditions limiting such assignment; conformance to occupational physical standards, where applicable; continued fitness for duty, suitability, and continuation of service at post (including decisions on curtailment); (b) separation medical examinations; and (c) determinations of eligibility of members of the Foreign Service for disability retirement (whether on application of the employee or the Secretary);

(3) of eligible family members of Foreign Service or other United States Government employees, for medical clearance determinations like those described in (2) above to permit such family members to accompany employees to posts abroad on Government orders, as well as determinations regarding family members remaining at post and separation medical examinations.

The proposed exemption is intended to maintain the DOS's procedures regarding internal of medical information in conformance with the Privacy Act of 1974, as amended, and 42 CFR Part 2, which would continue to apply to the DOS. The verification requirements of § 164.518(c) would apply to these disclosures.

The DOS is considering the need to add national security determinations under Executive Order 10450, as amended, and other suitability determinations to the exempted purposes listed above. We therefore request comment as to the purposes for which use or disclosure of protected health information without individual authorization by the DOS would be appropriate.

d. *Application to employees of the intelligence community.*

[*Please label comments about this section with the subject: ''Intelligence community''*]

We propose to permit covered entities to disclose protected health information about individuals who are employees of the intelligence community (as defined in Section 4 of the National Security Act, 50 U.S.C. 401a), and their dependents, to intelligence community agencies without individual authorization when authorized by law.

This provision addresses the special circumstances of the national intelligence community. The preservation of national security depends to a large degree on the health and well-being of intelligence personnel. To determine fitness for duty, including eligibility for a security clearance, these agencies must have continued access to the complete health records of their employees. To ensure continued fitness for duty, it is critical that these agencies have access to the entire medical record on a continuing basis. An incomplete medical file that excluded mental health information, for instance, could result in an improper job placement and a potential breach in security.

The term ''intelligence community'' is defined in section 4 of the National Security Act, 50 U.S.C. 401a, to include: the Office of the Director of Central Intelligence, which shall include the Office of the Deputy Director of Central Intelligence, the National Intelligence Council (as provided for in 50 U.S.C. 403–5(b)(3) [1]), and such other offices as the Director may designate; the Central Intelligence Agency; the National Security Agency; the Defense Intelligence Agency; the National Imagery and Mapping Agency; the National Reconnaissance Office; other offices within the DOD for the collection of specialized national intelligence through reconnaissance programs; the intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Federal Bureau of Investigation, the Department of the Treasury, and the Department of Energy; the Bureau of Intelligence and Research of the Department of State; and such other elements of any other department or agency as may be designated by the President, or designated jointly by the Director of Central Intelligence and the head of the department or agency concerned, as an element of the intelligence community.

We would permit covered entities to disclose protected health information concerning employees of the intelligence community and their dependents where authorized by law. The verification requirements of § 164.518(c) would apply to these disclosures.

F. Rights of individuals.

[*Please label comments about this section with the subject: ''Introduction to rights of individuals''*]

The following proposed sections are intended to facilitate individual understanding of and involvement in the handling of their protected health information. Four basic individual rights would be created under this section: the right to a notice of information practices; the right to obtain access to protected health information about them; the right to obtain access to an accounting of how their protected health information has been disclosed; and the right to request amendment and correction of protected health information.

The rights described below would apply with respect to protected health information held by health care providers and health plans. We are proposing that clearinghouses not be subject to all of these requirements. We believe that as business partners of covered plans and providers, clearinghouses would not usually initiate or maintain direct relationships with individuals. The contractual relationship between a clearinghouse (as a business partner) and a covered plan or provider would bind the clearinghouse to the notice of information practices developed by the plan or provider and it will include specific provisions regarding inspection, copying, amendment and correction. Therefore, we do not believe the clearinghouses should be required to provide a notice or provide access for inspection, copying, amendment or correction. We would require clearinghouses to provide an accounting of any disclosures for purposes other than treatment, payment and health care operations to individuals upon request. See proposed § 164.515. It is our understanding that the vast majority of the clearinghouse function falls within the scope of treatment, payment, and health care operations and therefore we do not believe providing this important right to individuals will impose a significant burden on the industry. We invite comment on whether or not we should require clearinghouses to comply with all of the provisions of the individual rights section.

1. *Rights and Procedures for a Written Notice of Information Practices.* (§ 164.512)

[*Please label comments about this section with the subject: ''Notice of information practices''*]

a. *Right to a written notice of information procedures.* We are proposing that individuals have a right to an adequate notice of the information practices of covered plans and providers. The notice would be intended to inform individuals about what is done with their protected health information and about any rights they may have with respect to that information. Federal agencies must adhere to a similar notice requirement pursuant to the Privacy Act of 1974 (5 U.S.C. 552a(e)(3)).

We are not proposing that business partners (including health care clearinghouses) be required to develop a notice of information practices because, under this proposed rule, they would be bound by the information practices of the health plan or health care provider with whom they are contracting.

We considered requiring covered plans or providers to obtain a signed copy of the notice form (or some other signed indication of receipt) when they give the form to individuals. There are advantages to including such a requirement. A signed acknowledgment would provide evidence that the notice form has been provided to the individual. Further, the request to the individual to formally acknowledgment receipt would highlight the importance of the notice, providing additional encouragement for the individual to

read it and ask questions about its content.

We are concerned, however, that requiring a signed acknowledgment would significantly increase the administrative and paperwork burden of this provision. We also are unsure of the best way for health plans to obtain a signed acknowledgment because plans often do not have face-to-face contact with enrollees. It may be possible to collect an acknowledgment at initial enrollment, for example by adding an additional acknowledgment to the enrollment form, but it is less clear how to obtain it when the form is revised. We solicit comment on whether we should require a signed acknowledgment. Comments that address the relative advantages and burdens of such a provision would be most useful. We also solicit comment on the best way to obtain signed acknowledgments from health plans if such a provision is included in the final rule. We also solicit comments on other strategies, not involving signed acknowledgments, to ensure that individuals are effectively informed about the information practices of covered plans or providers.

b. *Revising the notice.* We are proposing that covered plans and providers be permitted to change their policies and procedures at any time. Before implementing a change in policies and procedures, the covered plan or provider must revise its notice accordingly. However, where the covered plan or provider determines that a compelling reason exists to take an action that violates its notice, it may do so only if it documents the reason supporting the action and revises its notice within 30 days of taking such action. The distribution requirements that would apply when the notice has been materially revised are discussed in detail below.

c. *Content of the notice.* In § 164.512, we propose the categories of information that would be required in each notice of information practices, the specific types of information that would have to be included in each category, and general guidance as to the presentation of written materials. A sample notice is provided in the Appendix to this preamble. This sample notice is provided as an example of how the policies of a specific covered health care provider could be presented in a notice. Each covered health plan and health care provider would be required to create a notice that complies with the requirements of this proposed rule and reflects its own unique information practices. It does not indicate all possible information practices or all issues that could be addressed in the notice. Covered plans and providers may want to include significantly more detail, such as the business hours during which an individual could review their records or its standard time frame for responding to requests to review records; entities could choose to list all types of mandatory disclosures.

In a separate section of this proposed rule, we would require covered plans or providers to develop and document policies and procedures relating to use, disclosure, and access to protected health information. See proposed § 164.520. We intend for the documentation of policies and procedures to be a tool for educating the entity's personnel about its policies and procedures. In addition, the documentation would be the primary source of information for the notice of information practices. We intend for the notice be a tool for educating individuals served by the covered plan or provider about the information practices of that entity. The information contained in the notice would not be as comprehensive as the documentation, but rather provide a clear and concise summary of relevant policies and procedures.

We considered prescribing specific language that each covered plan or provider would include in its notice. The advantages of this approach would be that the recipient would get exactly the same information from each covered plan or provider in the same format, and that it would be convenient for covered plans or providers to use a uniform model notice.

There are, however, several disadvantages to this approach. First, and most important, no model notice could fully capture the information practices of every covered plan or provider. Large entities will have different information practices than small entities. Some health care providers, for example academic teaching hospitals, may routinely disclose identifiable health information for research purposes. Other health care providers may rarely or never make such disclosures. To be useful to individuals, each entity's notice of information practices should reflect its unique privacy practices.

Another disadvantage of prescribing specific language is that it would limit each covered plan or provider's ability to distinguish itself in the area of privacy protections. We believe that if information on privacy protections were readily available, individuals might compare and select plans or providers based on their information practices. In addition, a uniform model notice could easily become outdated. As new communication methods or technologies are introduced, the content of the notices might need to reflect those changes.

A covered plan or provider that adopts and follows the notice content and distribution requirements described below, we would presume, for the purposes of compliance, that the plan or provider has provided adequate notice. However, the proposed requirements for the content of the notice are not intended to be exclusive. Covered plans or providers could include additional information and additional detail, beyond that required. In particular, all federal agencies must still comply with the Privacy Act of 1974. For federal agencies that are covered plans or providers, this would mean that the notice must comply with the notice requirements provided in the Privacy Act as well as those included in this proposed rule.

i. *Uses and disclosures of protected health information.*

In proposed § 164.512, we would require each covered plan and provider to include in the notice an explanation of how it uses and discloses protected health information. The explanation must be provided in sufficient detail as to put the individual on notice of the uses and disclosures expected to be made of his or her protected health information. As explained above in section II.C.5, covered plans and providers may only use and disclose protected health information for purposes stated in this notice.

This section of the notice might be as simple as a statement that information will be used and disclosed for treatment, payment, administrative purposes, and quality assurance. If the entity will be using or disclosing the information for other purposes, the notice must include a brief explanation. For example, some entities might include a statement that protected health information will be used for clinician education and disclosed for research purposes. We are soliciting comment on the level of detail that should be required in describing the uses and disclosures, specifically with respect to uses and disclosures for health care operations.

In addition we would require that notices distinguish between those uses and disclosures the entity makes that are required by law and those that are permitted but not required by law. By distinguishing between uses and disclosures that an entity is required to make those that the entity is choosing to make, the notice would provide the

individual with a clearer understanding of the entity's privacy practices.

For uses and disclosures required by law, the notice need only list the categories of disclosures that are authorized by law, and note that it complies with such requirements. This language could be the same for every covered entity within a State, territory or other locale. We encourage states, state professional associations, and other organizations to develop model language to assist covered plans or providers in preparing this section of the notice.

For each type of permissible use or disclosure that the entity makes (e.g., research, public health, and next-of-kin), the notice would include a brief statement explaining the entity's policy with respect to that type of disclosure. For example, if all relevant laws permit health care providers to disclose protected health information to public health without individual authorization, the entity would need to develop policies and procedures regarding when and how it will make such disclosures. The entity would then document those policies and procedures as required by § 164.520 and the notice would include a statement of these policies. For example, the notice might state ''we will disclose your protected health information to public health authorities upon request.''

We considered requiring the notice to include not only a discussion the actual disclosure practices of the covered entity, but also a listing or discussion of all additional disclosures that are authorized by law. We considered this approach because, under this proposed rule, covered plans or providers would be permitted to change their information practices at any time, and therefore individuals would not be able to rely on the entity's current policies alone to understand how their protected health information may be used in the future. We recognize that in order to be fully informed, individuals need to understand when their information could be disclosed.

We rejected this approach because we were concerned that a notice with such a large amount of information could be burdensome to both the individuals receiving the notices and the entities required to prepare and distribute them. There are a substantial number of required and permitted disclosures under State or other applicable law, and this rule generally would permit them to be made.

Alternatively, we considered requiring that the notice include all of the types of permissible disclosures under this rule (e.g., public health, research, next-of-kin). We rejected that approach for two reasons. First, we felt that providing people with notice of the intended or likely disclosures of their protected health information was more useful than describing all of the potential types of disclosures. Second, in many States and localities, different laws may affect the permissible disclosures that an entity may make, in which case a notice only discussing permissible disclosures under the federal rule would be misleading. While it would be possible to require covered plans or providers to develop notices that discuss or list disclosures that would be permissible under this rule and other law, we were concerned that such a notice may be very complicated because of the need to discuss the interplay of federal, State or other law for each type of permissible disclosure. We invite comments on the best approach to provide most useful information to the individuals without overburdening either covered plans or providers or the recipients of the notices.

In § 164.520, we are proposing to require all covered entities to develop and document policies and procedures for the use of protected health information. The notice would simply summarize those documented policies and procedures and therefore would entail little additional burden.

ii. *Required statements.*

We are proposing that the notice include several basic statements to inform the individual of their rights and interests with respect to protected health information. First, we propose to require the notice to inform individuals that the covered plan or provider will not use or disclose their protected health information for purposes not listed in the notice without the individual's authorization. Individuals need to understand that they can authorize a disclosure of their protected health information and that the covered entity may request the individual to authorize a disclosure, and that such disclosures are subject to their control. The notice should also inform individuals that such authorizations can be revoked.

Second, we propose that the notice inform individuals that they have the right to request that the covered plan or provider restrict certain uses and disclosures of protected health information about them. The notice would also inform individuals that the covered plan or provider is not required to agree to such a request.

Third, we propose that the notice also inform individuals about their right of access to protected health information for inspection and copying and to an accounting of disclosures as provided in proposed §§ 164.514 and 164.515. In addition, the notice would inform individuals about their right to request an amendment or correction of protected health information as proposed in § 164.516. The notice would include brief descriptions of the procedures for submitting requests to the covered plan or provider.

Fourth, the notice would be required to include a statement that there are legal requirements that require the covered plan or provider to protect the privacy of its information, provide a notice of information practices, and abide by the terms of that notice. Individuals should be aware that there are government requirements in place to protect their privacy. Without this statement, individuals may not realize that covered plans or providers are required to take measures to protect their privacy, and may therefore be less interested in pursuing their rights or finding out more information.

Fifth, the notice would be required to include a statement that the entity may revise its policies and procedures with respect to uses or disclosures of protected health information at any time and that such a revision could result in additional uses or disclosures without the individual's authorization. The notice also should inform the individual how a revised notice would be made available when material revisions in policies and procedures are made. For example, when a provider makes a material change to its notice, proposed § 164.512(e) would require the provider to post a new notice.

Finally, we propose that the notice inform individuals that they have the right to complain to the covered entity and to the Secretary if they believe that their privacy rights have been violated.

iii. *Identification of a contact person for complaints and additional information.*

We propose that the notice be required to identify a contact person or office within the covered plan or provider to receive complaints, as provided in proposed § 164.518(a)(2), and to help the individual obtain further information on any of the issues identified in the notice. A specific person would not need to be named in the notice. It could be an office or general number where someone who can answer privacy questions or concerns can be reached.

In § 164.518(d), we are proposing that covered plans and providers permit individuals to submit complaints to the covered entity. We are proposing that the contact person identified in the

notice be responsible for initially receiving such complaints. The contact person might or might not be responsible for processing and resolving complaints, but, if not, he or she would forward the complaints to the appropriate personnel or office. See discussion of the complaint process in section II.G.4, below.

In addition to receiving complaints, the contact person would be able to help the individual obtain further information on any of the issues identified in the notice. The contact person would be able to refer to the documented policies and procedures required by proposed § 164.520. We would not prescribe a formal method for responding to questions.

The administrative requirements section below, proposed § 164.518(a), would also require the entity to designate an official to develop policies for the use and disclosure of protected health information and to supervise personnel with respect to use and disclosure of protected health information. We would not require this official to also be the contact person. Depending on the size and structure of the entity, it might be appropriate to require one person to fill both roles.

iv. *Date the notice was produced.*

We are proposing that covered plans and providers include the date that the notice was produced on the face of the notice. We would also encourage the provider to highlight or otherwise emphasize any changes to help the individual recognize such changes.

d. *Requirements for distribution of the notice.* It is critical to the effectiveness of this proposed rule that individuals be given the notice often enough to remind them of their rights, but without overburdening covered plans or providers. We propose that all covered plans and providers would be required to make their notice available to any individual upon request, regardless of whether the requestor is already a patient or enrollee. We believe that broad availability would encourage individuals or organizations to compare the privacy practices of plans or providers to assist in making enrollment or treatment choices. We also propose additional distribution requirements for updating notices, which would be different for health plans and health care providers. The requirements for health plans and health care providers are different because we recognize that they have contact with individuals at different points in time in the health care system.

i. *Health plans.*

We considered a variety of combinations of distribution practices for health plans and are proposing what we believe is the most reasonable approach. We would require health plans to distribute the notice by the effective date of the final rule, at enrollment, within 60 days of a material change to the plan's information practices, and at least once every three years.

We considered requiring health plans to post the notice either in addition to or instead of distribution. Because most individuals rarely visit the office of their health plan, we do not believe that this would be an effective means of communication. We also considered either requiring distribution of the notice more or less frequently than every three years. As compared to most health care providers, we believe that health plans often are larger and have existing administrative systems to cost effectively provide notification to individuals. Three years was chosen as a compromise between the importance of reminding individuals of their plans' information practices and the need to keep the burden health plans to the minimum necessary to achieve this objective. We are soliciting comment on whether requiring a notice every three years is reasonable for health plans.

ii. *Health care providers.*

We are proposing to require that covered health care providers provide a copy of the notice to every individual served at the time of first service delivery, that they post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the provider to be able to read the notice, and that copies be available on-site for individuals to take with them. In addition, we are proposing to require that covered health care providers provide a copy of the notice to individuals they are currently serving at their first instances of service delivery within a year of the effective date of the final rule.

We would not require health care providers to mail or otherwise disseminate their notices after giving the notice to individuals at the time of the first service delivery. Health care providers' patient lists may include individuals they have not served in decades. It would be difficult for providers to distinguish between ''active'' patients, those who are seen rarely, and those who have moved to different providers. While some individuals will continue to be concerned with the information practices of providers who treated them in the distant past, overall the burden of an active distribution requirement would not be outweighed by improved individual control and privacy protection.

We recognize that some health care providers, such as clinical laboratories, pathologists and mail order pharmacies, do not have face-to-face contact with individuals during service delivery. Such providers would be required to provide the required notice in a reasonable period of time following first service delivery, through mail, electronic notice (i.e. e-mail), or other appropriate medium. For example, a web-based pharmacy could meet this distribution requirement by providing a prominent and conspicuous link to its notice on its home page and by requiring review of that notice before processing an order.

If a provider wishes to make a material change in the information practices addressed in the notice, it would be required to revise its notice in advance. After making the revision, the provider would be required to post the new notice promptly. We believe that this approach creates the minimum burden for health care providers consistent with giving individuals a clear source of accurate information.

e. *Plain language requirement.* We are proposing to apply a plain language requirement to notices developed by covered plans or providers under these proposed rules. A covered plan or provider could satisfy the plain language requirement if it made a reasonable effort to: organize material to serve the needs of the reader; write sentences in the active voice, use ''you'' and other pronouns; use common, everyday words in sentences; write in short sentences; and divide material into short sections.

We also considered proposing formatting specifications such as requiring the covered plan or provider to use easy-to-read design features (e.g., lists, tables, graphics, contrasting colors, and white space), type face, and font size in the notice. We are soliciting comment on whether these additional format specifications should be required.

The purpose of the notice proposed in the rules below is to tell the recipient how protected health information collected about them will be used. Recipients who cannot understand the entity's notice would miss important information about their privacy rights and how the entity is protecting health information about them. One of the goals of this proposed rule is to create an environment of open communication and transparency with respect to the use and disclosure of protected health information. A lack of clarity in the notice could undermine this goal and

create misunderstandings. Covered plans or providers have an incentive to make their notice statements clear and concise. We believe that the more understandable notices are, the more confidence the public will have in the entity's commitment to protecting the privacy of health information.

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

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

The requirement of a printed notice should not be interpreted as a limitation. For example, if an individual who is requesting a notice from a covered plan or providers were to ask to receive the notice via e-mail, the requirements of this proposed rule could be met by providing the notice via e-mail. The proposed rule would not preclude the use of alternative forms of providing the notice and we would encourage covered plans or providers to use other forms of distribution, such as posting their privacy notices on their web sites. While this will not substitute for paper distribution when that is requested by an individual, it may reduce the number of requests for paper copies.

2. Rights and Procedures for Access for Inspection and Copying (§ 164.514)

a. *Right of access for inspection or copying.* (§ 164.514(a))

[Please label comments about this section with the subject: ''Access for inspection or copying'']

In § 164.514, we are proposing that, with very limited exceptions, individuals have a right to inspect and copy protected health information about them maintained by a covered health plan or health care provider in a designated record set. Individuals would also have a right of access to protected health information in a designated record set that is maintained by a business partner of a covered plan or provider when such information is not a duplicate of the information held by the plan or provider, including when the business partner is the only holder of the information or when the business partner has materially altered the protected health information that has been provided to it.

This right of access means that an individual would be able to either inspect or obtain copies of his or her health information maintained in a designated record set by covered plans and providers and, in limited circumstances, by their business partners. Inspection and copying is a fundamental aspect of protecting privacy; this right empowers individuals by helping them to understand the nature of the health information about them that is held by their providers and plans and to correct errors. In order to facilitate an open and cooperative relationship with providers and allow the individual a fair opportunity to know what information is held by an entity, inspection and copying should be permitted in almost every case.

While the right to have access to one's information may appear somewhat different from the right to keep information private, these two policy goals have always been closely tied. For example, individuals are given an almost absolute right of access to information in federal health record systems under the Privacy Act of 1974 (5 U.S.C. 552a(d)). The Privacy Protection Study Commission recommended that this right be available. (Personal Privacy in an Information Society 299 (1977)). The right of access was a key component of the President's Advisory Commission on Consumer Protection and Quality in the Health Care Industry recommendations in the Consumer Bill of Rights and Responsibilities. The Commission's report stated that consumers should ''have the right to review and copy their own medical records and request amendments to their records.'' (Consumer Bill of Rights and Responsibilities, Chapter Six: Confidentiality of Health Information, November 1997). Most recently, the Health Privacy Project issued a statement of ''Best Principles for Health Privacy'' that included the same recommendation. Health Privacy Project, Institute for Health Policy Solutions, Georgetown University (June 1999) (http://www.healthprivacy.org).

Open access to health information can benefit both the individuals and the covered entities. It allows individuals to better understand their own diagnosis and treatment, and to become more active participants in their health care. It can increase communication, thereby enhancing individuals' trust in their health care providers and increasing compliance with the providers' instructions. If individuals have access to and understand their health information, changing providers may not disrupt health care or create risks based on lack of information (e.g., drug allergies or unnecessary duplication of tests).

i. *Information available for inspection and copying.*

In § 164.514(a), we are proposing to give the individual a right of access to information that is maintained in a designated record set. We intend to provide a means for individuals to have access to any protected health information that is used to affect their rights and interests. This would include, for example, information that would be used to make health care decisions or information that would be used in determining whether an insurance claim would be paid. Covered plans or providers often incorporate the same protected health information that is used to make these types of decisions into a variety of different data systems. Not all of those data systems will be utilized to make determinations about specific individuals. For example, information systems that are used for quality control analyses are not usually used to make determinations about a specific patient. We would not require access to these other systems.

In order to ensure that individuals have access to the protected health information that is used, we are introducing the concept of a ''designated record set.'' In using the term ''designated record set,'' we are drawing on the concept of a ''system of records'' that is used in the Privacy Act. Under the Privacy Act, federal agencies must provide an individual with access to ''information pertaining to him which

is contained in (a system of records).'' 5 U.S.C. 552a(d)(1). A ''system of records'' is defined as ''a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.'' 5 U.S.C. 552a(a)(5). Under this rule, a ''designated record set'' would be ''a group of any records under the control of any covered entity from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.'' See discussion in section II.B.

Files used to backup a primary data system or the sequential files created to transmit a batch of claims to a clearinghouse are clear examples of data files which do not fall under this definition. We rejected requiring individual access to all records in which she or he was identifiable because of the extreme burden it would place on covered plans or providers without providing additional information or protection for the individual. We also rejected using the subset of such records which were accessed directly by individual identifiers because of the redundancy of information involved and the increasing use of database management systems to replace legacy systems that do sequential processing. These would be accessed by individual identifier but would contain redundant data and be used for routine processing that did not directly affect the individual. We concluded that access to only such record sets that were actually accessed by individual identifier and that were used to make substantive decisions that affect individuals would provide the desired information with a minimum of burden for the covered plans or providers.

We note that the standard would apply to records that are ''retrieved'' by an identifier and not records that are only ''retrievable'' by an identifier. In many cases, technology will permit sorting and retrieving by a variety of fields and therefore the ''retrievable'' standard would be relatively meaningless. We intend to limit access to those sets of records actually used to affect the interests of the individual.

We believe that by providing access to protected health information maintained in a designated record set, we would be ensuring that individuals will be able to inspect or copy relevant and appropriate information without placing too significant of a burden on covered plans or providers. We are soliciting comment on whether limiting access to information maintained in a designated record set is an appropriate standard when applied to covered plans and providers and their business partners.

ii. *Right of access to information maintained by business partners.*

In § 164.506(e), we are proposing that covered plans and providers include specific terms in their contract with each business partner. One of the required terms would be that the business partner must provide for inspection and copying of protected health information as provided in this section. Because our authority is limited by HIPAA to the covered entities, we must rely upon covered plans and providers to ensure that all of the necessary protected health information provided by the individual to the plan or provider is available for inspection and copying. We would require covered plans and providers to provide access to information held in the custody of a business partner when it is different from information maintained by the covered plan or provider. We identified two instances where this seemed appropriate: when the protected health information is only in the custody of a business partner and not in the custody of the covered plan or provider; and when protected health information has been materially altered by a business partner. We are soliciting comment on whether there are other instances where access should be provided to protected health information in the custody of a business partner.

Other than in their capacity as business partners, we are not proposing to require clearinghouses to provide access for inspection and copying. As explained above in section II.C.5, clearinghouses would usually be business partners under this proposed rule and therefore they would be bound by the contract with the covered plan or provider. See proposed § 164.506(e). We carefully considered whether to require clearinghouses to provide access for inspection and copying above and beyond their obligations as a business partner, but determined that the typical clearinghouse activities of translating record formats and batching transmissions do not involve setting up designated record sets on individuals. Although the data maintained by the clearinghouse is protected health information, it is normally not accessed by individual identifier and an individual's records could not be found except at great expense. In addition, although clearinghouses process protected health information and discover errors, they do not create the data and make no changes in the original data. They, instead, refer the errors back to the source for correction. Thus, individual access to clearinghouse records provides no new information to the individual but could impose a significant burden on the industry.

As technology improves it is likely that clearinghouses will find ways to take advantage of databases of protected health information that aggregate records on the basis of the individual subject of the information. This technology would allow more cost-effective access to clearinghouse records on individuals and therefore access for inspection and copying could be appropriate and reasonable.

iii. *Duration of the right of access.*

We are proposing that covered plans and providers be required to provide access for as long as the entity maintains the protected health information. We considered requiring covered plans and providers to provide access for a specific period or defining a specific retention period. We rejected that approach because many laws and professional standards already designate specific retention periods and we did not want to create unnecessary confusion. In addition, we concluded that individuals should be permitted to have access for as long as the information is maintained by the covered plan or provider. We are soliciting comments on whether we should include a specific duration requirement in this proposed rule.

b. *Grounds for denial of access for inspection and copying.* Proposed § 164.514 would permit denial of inspection and copying under very limited circumstances. The categories of denials would not be mandatory; the entity could always elect to provide all of the requested health information to the individual. For each request by an individual, the entity could provide all of the information requested or it could evaluate the requested information, consider the circumstances surrounding the individual's request, and make a determination as to whether that request should be granted or denied. We intend to create narrow exceptions to the stated rule of open access and we would expect covered plans and providers to employ these exceptions rarely, if at all.

In proposing these categories of permissible denials, we are not intending to create a legal duty for the entity to review all of the health information before releasing it. Rather, we are proposing them as a means of preserving the flexibility and judgment of covered plans or providers under appropriate circumstances.

Entities subject to the Privacy Act would not be able to deny a request for inspection and copying under all of the circumstances permitted by this proposed rule. They would continue to be governed by the denials permitted by the Privacy Act and applicable regulations. See section II.I.4.a for further discussion.

i. *Disclosures reasonably likely to endanger life or physical safety.*

In § 164.514(b)(1)(i), we propose that covered plans and providers be permitted to deny a request for inspection or copying if a licensed health care professional has determined that, in the exercise of reasonable professional judgment, the inspection and copying requested is reasonably likely to endanger the life or physical safety of the individual or another person. Denial based on this provision, as with all of the provisions in this section, would be discretionary. While it is important to protect the individual and others from physical harm, we are also concerned about the subjectivity of the standard and are soliciting comments on how to incorporate a more objective standard into this provision.

We are proposing that covered plans and providers should only consider denying a request for inspection and copying under this provision in situations where a licensed health care professional (such as a physician, physician's assistant or nurse) makes the determination that access for inspection and copying would be reasonably likely to endanger life or physical safety. We are proposing to require a licensed health care professional to make the determination because it would rely entirely on the existing standards and ethics in the medical profession. In some instances, the covered plan or provider would be a licensed health care professional and therefore, he or she could make the determination independently. However, when the request is made to a health plan, the entity would need to consult with a health care professional in order to deny access under this provision.

We are soliciting comments as to whether the determination under this provision should be limited to health care professionals who have an existing relationship with the individual. While such a limitation would significantly restrict the scope of this provision and could reduce the number of denials of requests for inspection and copying, it could also ensure that the determination of potential harm is as accurate as possible.

By proposing to allow covered plans and providers to deny a request for inspection and copying based on potential endangerment, we are not suggesting that entities should deny a request on that basis. This provision is not intended to be used liberally as a means of denial of individual inspection and copying rights for all mental health records or other ''sensitive'' health information. Each request for access would have to be assessed on its own merits. We would expect the medical community to rely on its current professional standards for determining what constitutes a threat to life or physical safety.

As explained above, we are not proposing to create a new ''duty'' whereby entities can be held liable for failure to deny inspection and copying. We simply are acknowledging that some providers, based on reasonable professional judgment, may already assume a duty to protect an individual from some aspect of their health information because of the potential for physical harm. The most commonly cited example is when an individual exhibits suicidal or homicidal tendencies. If a health care professional determines that an individual exhibits such tendencies and that permitting inspection or copying of some of their health information could reasonably result in the individual committing suicide, murder or other physical violence, then the individual could be denied access to that information.

We considered whether covered plans and providers should be permitted to deny access on the basis of sensitivity of the health information or the potential for causing emotional or psychological harm. Many States allow denial of access on similar grounds. In balancing the desire to provide individual access against the need to protect the individual, we concluded that the individual access should prevail because in the current age of health care , it is critical that the individual is aware of his or her health information.

Therefore, if a health care professional determines that inspection and copying of the requested information may cause emotional or psychological harm, but is not reasonably likely to endanger the life or physical safety of the individual or another person, then the covered plan or provider would not be permitted to deny the individual's request. If the entity is concerned about the potential for emotional or psychological harm, we would encourage it to offer special procedures for explaining the information or counseling the individual. For example, an entity could offer to have a nurse or other employee review the information or the format with the individual or provide supplemental written materials explaining a diagnosis. If the entity elects to offer such special procedures, the entity would not be permitted to condition inspection and copying upon compliance with the procedures. We are not proposing to require covered plans or providers to establish any informational or counseling procedures and we are not proposing that individuals be required to comply with any procedures in order to obtain access to their protected health information. We invite comment on whether a standard such as emotional distress or psychological harm should be included as a reason for which a covered plan or provider could deny a request for inspection or copying.

ii. *Disclosures likely to cause harm to another individual.*

We propose that covered plans and providers be permitted to deny a request for inspection or copying if the information requested is about another person (other than a health care provider) and a licensed health care professional has determined that inspection or copying is reasonably likely to cause substantial harm to that other person. We believe that it is rare that information about one person would be maintained within the health records of another without one or both of their knowledge. On some occasions when health information about one person is relevant to the care of another, a physician may incorporate it into the latter's record, such as information from group therapy sessions and illnesses with a genetic component. In some instances the information could be shared without harm, or may already be known to the individual. There may, however, be situations where disclosure could harm the other person, such as by implicitly revealing facts about past sexual behavior, nonpaternity, or similarly sensitive information. This provision would permit withholding of information in such cases.

We believe that this determination should be based on the existing standards and ethics in the medical profession. We are soliciting comments on whether the determination under this provision should be limited to health care professionals who have an existing relationship with the person who is expected to be harmed as a result of the inspection or copying.

Information about a third party may appear in an individual's records unbeknownst to the individual. In such cases if the individual chooses to exercise her right to inspect her protected health information, the covered plan or provider providing her access would be making an

unauthorized disclosure unless the third party has provided a written authorization. We considered requiring that access to such information be denied because the third party had not provided an authorization. We considered proposing that the covered plan or provider would be required to deny an individual's request for access to any information about another person, unless there was a potential for harm to the individual who would be denied. This would have been the only instance where we would require that access be denied as a general rule. We recognized that such requirements would ultimately require covered plans and providers to review every piece of protected health information before permitting inspection and copying to determine if information about another person was included and whether the requester would be harmed without such information. We concluded that this would impose a significant burden on covered plans and providers. We seek comment on whether and how often individual health records contain identifiable information about other persons, and current practice relating to the handling of such information in response to individual requests for access.

iii. *Disclosures of confidential information likely to reveal the source.*

We propose that covered plans or providers be permitted to deny a request for inspection and copying if the entity determines that the requested information was obtained under a promise of confidentiality from someone other than a health care provider and such access would be likely to reveal the source of the information. This provision is intended to preserve an entity's ability to maintain an implicit or explicit promise of confidentiality.

Covered plans and providers would not be permitted to deny access when the information has been obtained from another health care provider. An individual is entitled to have access to all information about him or her generated by the health care system (apart from the other exceptions we propose here), and confidentiality promises by health care providers to other providers should not interfere with that access.

iv. *Disclosures of clinical trial information.*

While a clinical trial is research, it is also health care as defined in § 160.103, and the information generated in the course of the trial would be protected health information. In § 164.514(b)(iv), we are proposing that a researcher/provider could deny a request for inspection and copying of the clinical trial record if the trial is still in progress, and the subject-patient had agreed to the denial of access in conjunction with the subject's consent to participate in the trial. The IRB or privacy board would determine whether such waiver of access to information is appropriate, as part of its review of the research protocol. In the rare instances in which individuals are enrolled in trials without consent (such as those permitted under FDA regulations, at 21 CFR 50.23), the covered entity could deny access to information during the course of the trial even without advance subject consent.

Clinical trials are often masked—the subjects do not know the identity of the medication they are taking, or of other elements of their record while the trial is in progress. The research design precludes their seeing their own records and continuing in the trial. Thus it is appropriate for the patient to waive the right to see the record while the trial is in progress. This understanding would be an element of the patient's consent to participate in the trial; if the consent signed by the patient did not include this fact, the patient would have the normal right to see the record. In all cases, the subject would have the right to see the record after the trial is completed.

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

v. *Disclosure of information compiled for a legal proceeding.*

In § 164.514(b)(1)(v), we are proposing that covered plans and providers be permitted to deny a request for inspection and copying if the information is compiled in reasonable anticipation of, or for use in, a legal proceeding. This provision would permit the entity to deny access to any information that relates specifically to legal preparations but not to the individual's underlying health information. For example, when a procedure results in an adverse outcome, a hospital's attorney may obtain statements or other evidence from staff about the procedure, or ask consultants to review the facts of the situation for potential liability. Any documents containing protected health information that are produced as a result of the attorney's inquiries could be kept from the individual requesting access. This provision is intended to incorporate the attorney work-product privilege. Similar language is contained in the Privacy Act and has been interpreted to extend beyond attorneys to information prepared by ''lay investigators.''

We considered limiting this provision to ''civil'' legal proceedings but determined that such a distinction could create difficulties in implementation. In many situations, information is gathered as a means of determining whether a civil or criminal violation has occurred. For example, if several patients were potentially mistreated by a member of a provider's staff, the provider may choose to get copies of the patients' records and interview other staff members. The provider may not know at the time they are compiling all of this information whether any investigation, civil or criminal, will take place. We are concerned that if we were to require the entity to provide the individual with access to this information, we might unreasonably interfere with this type of internal monitoring.

c. *Provision of other protected health information where access for inspection and copying is denied.* In proposed § 164.514(b)(2), we would require a covered plan or provider that elects to deny a request for inspection or copying as provided above to make any other protected health information requested available to the individual to the extent possible consistent with the denial. The plan or provider could redact or otherwise exclude only the information that falls within one or more of the denial criteria described above and would be required to permit inspection and copying of all remaining information. This provision is key to the right to inspect and copy one's health information. We intend to create narrow exceptions to the stated rule of open access for inspection and copying and we would expect covered plans or providers to employ these exceptions rarely, if at all. In the event that a covered plan or provider would find it necessary to deny access, then the denial would need to be as limited in scope as possible.

d. *Procedures to effect right of access for inspection and copying.* In § 164.514(c) and (d), we are proposing that covered plans and providers be required to have procedures that enable individuals to exercise their rights to inspect and obtain a copy of protected health information as explained above.

We considered whether this proposed rule should include detailed procedures governing a individual's request for inspection and copying. Because this proposed rule will affect such a wide range of entities, we concluded that it should only provide general guidelines and that each entity should have the discretion to develop procedures consistent with its own size, systems, and operations.

i. *Time limits.*

In § 164.514(d)(2), we are proposing that the covered plans and providers would take action upon the request as soon as possible but not later than 30 days following receipt of the request. We considered the possibility of not including a time limitation but rather imposing a ''reasonableness'' requirement on the covered plans or providers. We concluded that the individual is entitled to know when to expect a response. This is particularly important in the context of health information, where an individual may need access to his or her information in order to make decisions about care. Therefore, in order to determine what would be ''reasonable,'' we examined the time limitations provided in the Privacy Act, the Freedom of Information Act (FOIA), and several State laws.

If the entity had fulfilled all of its duties under this proposed rule within the required time period, then the entity should not be penalized for any delay by the individual. For example, if, within the 30 days, a provider approves a request for inspection and copying, makes copies of the requested information, and notifies the individual that this information is available to be picked up and paid for at the provider's office, then the provider's duty would be discharged under the rule. The individual might not be able to pick up the information for another two weeks, but this extra time should not be counted against the provider.

The Privacy Act requires that upon receipt of a request for amendment (not access), the agency would send an acknowledgment to the individual within 10 working days. (5 U.S.C. 552a (d)(2)). We considered several options that included such an acknowledgment requirement. An acknowledgment would be valuable because it would assure the individual that their request was received. Despite the potential value of requiring an acknowledgment, we concluded that it could impose a significant administrative burden on some of the covered plans and providers. This proposed rule will cover a wide range of entities with varying capacities and therefore, we are reluctant to create requirements that would overwhelm smaller entities or interfere too much with procedures already in place. We would encourage plans and providers to have an acknowledgment procedure in place, but would not require it at this point. We are soliciting comment on whether this proposed rule should require such an acknowledgment.

We also considered whether to include specific procedures governing ''urgent'' or ''emergency'' requests. Such procedures would require covered plans and providers to respond in a shorter time frame. We recognize that circumstances may arise where an individual will request inspection and copying on an expedited basis and we encourage covered plans or providers to have procedures in place for handling such requests. We are not proposing additional regulatory time limitations to govern in those circumstances. The 30-day time limitation is intended to be an outside deadline, rather than an expectation. Rather, we would expect a plan or provider to always be attentive to the circumstances surrounding each request and respond in an appropriate time frame, not to exceed 30 days.

Finally, we considered including a section governing when and how an entity could have an extension for responding to a request for inspection and copying. For example, the FOIA provides that an agency may request additional time to respond to a request if the agency needs to search for and collect the requested records from facilities that are separate from the office processing the request; to search for, collect, and appropriately examine a voluminous amount of separate and distinct records; and to consult with another entity or component having a substantial interest in the determination of the request. We determined that the criteria established in the FOIA are tailored to government information systems and therefore may not be appropriate for plans and providers covered by this proposed rule. Furthermore, we determined that the 30-day time period would be sufficient for responding to requests for inspection and copying and that extensions should not be necessary. We are soliciting comments on whether a structured extension procedure should be included in this proposed rule.

ii. *Notification of accepted requests.*

In § 164.514(d)(3), we are proposing that covered plans or providers be required to notify the individual of the decision to provide access and of any steps necessary to fulfill the request. In addition we propose that the entity provide the information requested in the form or format requested if it is readily producible in such form or format. Finally, if the covered plan or provider accepts an individual's request, it would be required to facilitate the process of inspection and copying.

For example, if the plan or provider will be making copies and sending them directly to the individual with an invoice for copying costs, then it would need to ensure that the individual is aware of this procedure in advance and then send the information within the 30-day time period. If the plan or provider has procedures that require the individual to inspect the health information on site, then in addition to notifying the individual of the procedure, the entity would need to ensure that there are representatives available during reasonable business hours at the usual business address who can assist with inspection and copying. If the plan or provider maintains health information electronically and the individual requests an electronic copy, the plan or provider would need to accommodate such request if possible.

iii. *Copying fees.*

In proposed § 164.514(d)(3)(iv), we would permit a covered plan or provider to charge a reasonable, cost-based fee for copying health information provided pursuant to this section. We considered whether we should follow the practice in the FOIA and include a structured fee schedule. We concluded that the FOIA was developed to reflect the relatively uniform government costs and that this proposed rule would apply to a broader range of entities. Depending on the size of the entity, copying costs could vary significantly. Therefore, we propose that the entity simply charge a reasonable, cost-based fee.

The inclusion of a fee for copying is not intended to impede the ability of individuals to copy their records. Rather, it is intended to reduce the burden on covered plans and providers. When establishing a fee for copying, we encourage covered plans and providers to consider the impact on individuals of such a cost. If the cost is excessively high, some individuals would not be able to obtain a copy. We would encourage covered plans or providers to make efforts to keep the fee for copying within reach of all individuals.

iv. *Statement of denial of access for inspection and copying.*

In § 164.514(d)(4), we propose that a covered plan or provider that denies an individual's request for inspection and copying in whole or in part be required to provide the individual with a written statement in plain language explaining the reason for the denial. The statement could include a direct reference to the section of the regulation relied upon for

the denial, but the regulatory citation alone would not sufficiently explain the reason for the denial. The statement would need to include the name and number of the contact person or office within the entity who is responsible for receiving complaints. In addition, the statement would need to include information regarding the submission of a complaint with the Department pursuant to § 164.522(b).

We considered proposing that covered plans and providers provide a mechanism for appealing a denial of inspection and copying. We believe, however, that the requirement proposed in § 164.518(d) that covered plans and providers have complaint procedures to address patient and enrollee privacy issues generally would allow the individual to raise the issue of a denial with the covered plan or provider. We would expect the complaint procedures to be scalable; for example, a large plan might develop a standard complaint process in each location where it operates whereas, a small practice might simply refer the original request and denial to the clinician in charge for review. We would encourage covered plans and providers to institute a system of appeals, but would not require it by regulation. In addition, the individual would be permitted to file a complaint with the Department pursuant to § 164.522(b).

3. Rights and Procedures With Respect to an Accounting of Disclosures. (§ 164.515)

[*Please label comments about this section with the subject: ''Accounting of disclosures''*]

a. *Right to accounting of disclosures.* In this rule, we propose that individuals have a right to receive an accounting of all instances where protected health information about them is disclosed by a covered entity for purposes other than treatment, payment, and health care operations, subject to certain time-limited exceptions for disclosures to law enforcement and oversight agencies as discussed below. Providing such an accounting would allow individuals to understand how their health information is shared beyond the basic purposes of treatment, payment and health care operations.

We considered whether to require covered entities to account for all disclosures, including those for treatment, payment and health care operations. We rejected this approach because it would be burdensome and because it would not focus on the disclosures of most interest to individuals. Upon entering the health care system, individuals are generally aware that their information will be used and shared for the purpose of treatment, payment and health care operations. They have the greatest interest in an accounting of circumstances where the information was disclosed for other purposes that are less easy to anticipate. For example, an individual might not anticipate that his or her information would be shared with a university for a research project, or would be requested by a law enforcement agency.

We are not proposing that covered entities include uses and disclosures for treatment, payment and health care operations in the accounting. We believe that it is appropriate for covered entities to monitor all uses and disclosures for treatment, payment and health care operations, and they would be required to do so for electronically maintained information by the Security Standard. However, we do not believe that covered entities should be required to provide an accounting of the uses and disclosures for treatment payment and health care operations.

The proposed Security Standard would require that ''[e]ach organization * * * put in place audit control mechanisms to record and examine system activity. They would be important so that the organization can identify suspect data access activities, assess its security program, and respond to potential weaknesses.'' The purpose of the audit control mechanism, or audit trail, in the Security Standard would be to provide a means for the covered entity to police access to the protected health information maintained in its systems. By contrast, the purpose of the accounting would be to provide a means for individuals to know how the covered entity is disclosing protected health information about them. An audit trail is critical to maintaining security within the entity and it could be constructed in such a way to enable the covered plan or provider to satisfy the requirements of both regulations. For example, every time protected health information was used or disclosed, the audit mechanism could prompt the user for a ''purpose.'' If the disclosure was for a purpose other than treatment, payment or health care operations, then the information could be flagged or copied into a separate database. This would allow the entity to both monitor security and have the ability to provide an accurate accounting upon request.

Covered entities should know how all protected health information is used and disclosed, but should not be required to provide an exhaustive accounting of all uses and disclosures to individuals upon request. Such an accounting could be extremely long and detailed. It would place a tremendous burden on the covered entities and it could be far too detailed to adequately inform the individual. We determined that when individuals seek health care, they understand that information about them will be used and disclosed in order to provide treatment or obtain payment and therefore, they would have the most significant interest in knowing how protected health information was used and disclosed beyond the expected realm of treatment, payment and health care operations. We are soliciting comment on whether the scope of accounting strikes an appropriate balance between providing information to the individual and imposing requirements on covered entities.

We are proposing that covered entities be required to provide an accounting of disclosures for as long as the entity maintains the protected health information. We considered only requiring the accounting for a specified period of time, but concluded that individuals should be permitted to learn how their information was disclosed for as long as the information is maintained by the covered plan or provider. We are soliciting comments on whether we should include a specific time period in this proposed rule.

b. *Procedures for providing an accounting of disclosures.*

i. *Form or format.*

This proposed rule does not specify a particular form or format for the accounting. In order to satisfy the accounting requirement, a covered entity could elect to maintain a systematic log of disclosures or it could elect to rely upon detailed record keeping that would permit the entity to readily reconstruct the history when it receives a request from an individual. We would require that covered entities be able to respond to a request for accounting within a reasonable time period. In developing the form or format of the accounting, covered entities should adopt policies and procedures that will permit them to respond to requests within the 30-day time period in this proposed rule.

ii. *Content of the accounting of disclosures.*

We are proposing that the accounting include all disclosures for purposes other than treatment, payment, and health care operations, subject to certain exceptions for disclosures to law enforcement and oversight agencies, discussed below. This would also include disclosures that are authorized by the individual. The accounting would include the date of each disclosure; the name and address of the

organization or person who received the protected health information; and a brief description of the information disclosed. For all disclosures that are authorized by the individual, we are proposing that the covered entity maintain a copy of the authorization form and make it available to the individual with the accounting.

We considered whether the accounting of disclosures should include the name of the person who authorized the disclosure of information. The proposed Security Standard would require covered entities to have an audit mechanism in place to monitor access by employees. We concluded that it was unnecessary and inappropriate to require the covered entity to include this additional information in the accounting. If the individual identifies an improper disclosure by an entity, he or she should hold the entit—not the employee of the entity—accountable. It is the responsibility of the entity to train its workforce about its policies and procedures for the disclosure of protected health information and to impose sanctions if such policies and procedures are violated.

We are proposing that protected health information that is disclosed to a health oversight or law enforcement agency would be excluded from the accounting if the oversight or law enforcement agency provides a written request stating that the exclusion is necessary for a specified time period because access by the individual during that time period would be reasonably likely to impede the agency's activities. The written request must specifically state how long the information should be excluded. At the expiration of that period, the covered entity would be required to include the information in an accounting for the individual.

We are proposing this time-limited exclusion for law enforcement and oversight activities because we do not intend to unreasonably interfere with investigations and other activities that are in the public interest. The Recommendations simply provide that disclosures to law enforcement and oversight agencies should be excluded from the accounting where access by the individual could be reasonably likely to impede the agency's activities. We were concerned that it would be difficult for covered entities to determine whether access by the individual was ''reasonably likely to impede the agency's activities.'' In order to address this concern, we considered excluding all disclosures to law enforcement and oversight from the accounting, but concluded that such an exclusion would be overly broad. As a means of creating a clearly defined rule for the covered entity to follow, we are proposing that covered entities require a time-limited, written statement from the oversight or law enforcement agency. We are soliciting comment on whether this time-limited exclusion strikes the appropriate balance between ensuring individual access to an accounting of disclosures and preserving the integrity of law enforcement and oversight investigations.

iii. *Time limits.*

We are proposing that the accounting of disclosures, including copies of signed authorization forms, be made available to the individual as quickly as the circumstances require, but not later than 30 days following receipt of the request.

4. Rights and Procedures for Amendment and Correction (§ 164.516)

[*Please label comments about this section with the subject: ''Amendment or correction''*]

a. *Right to request amendment or correction of protected health information.* This proposed rule would provide an individual with the right to request a covered plan or provider to amend or correct protected health information relating to the individual. A covered plan or provider would be required to accommodate requests with respect to any information that the covered plan or provider determines to be erroneous or incomplete, that was created by the plan or provider, and that would be available for inspection and copying under proposed § 164.514.

i. *Accuracy and completeness.*

The first criteria that a covered entity would need to consider is whether the protected health information at issue is either erroneous or incomplete. The basic concept comes from the Privacy Act of 1974, governing records held by Federal agencies, which permits an individual to request correction or amendment of a record ''which the individual believes is not accurate, relevant, timely, or complete.'' (5 U.S.C. 552a(d)(2)). We would adopt the standards of ''accuracy'' and ''completeness'' and draw on the clarification and analysis of these terms that has emerged in administrative and judicial interpretations of the Privacy Act over the last 25 years.

We are not proposing to permit correction on the basis of an individual's belief that information is irrelevant or untimely. The Privacy Act of 1974 imposes affirmative obligations on Federal agencies to maintain records with accuracy, relevance, timeliness, and completeness, and permits individuals to seek correction of records that do not meet that standard. The amendment and correction right complements and helps to enforce the agency obligation.

Our view is that the relevance and timeliness standards, while very appropriate for Federal agencies generally, would be difficult to impose by regulation upon health record keeping, which depends to a large extent on clinical judgment. The increasingly-recognized impact of lifestyle and environmental factors on health may, for example, motivate physicians to record information which appears irrelevant, but which may in fact serve as a diagnostic clue, or which may alert later users of the record to clinically relevant aspects of the patient's life. We invite comment on how any such standard might be structured to avoid interfering inappropriately with clinical judgment.

We also are concerned about the burden that requests for amendment or correction may place on covered plans and providers and have tried to limit the process to those situations where amendment or correction would appear to be most important. We invite comment on whether our approach reasonably balances burden with adequately protecting individual interests.

We note that for Federal agencies that are also covered plans or providers, the rule we are proposing would not diminish their present obligations under the Privacy Act of 1974, under which all four factors are bases for amendment and correction.

ii. *Original creator of the information.*

We propose to require a covered plan or provider to accommodate a request for amendment or correction if the plan or provider created the information in dispute.

We considered requiring covered plans and providers to amend or correct any erroneous or incomplete information it maintains, regardless of whether it created the information. Under this approach, if the plan or provider did not create the information, then it would have been required to trace the information back to the original source to determine accuracy and completeness. We rejected this option because we concluded that it would not be appropriate to require the plan or provider that receives a request to be responsible for verifying the accuracy or completeness of information that it did not create. We also were concerned about the burden that would be imposed on covered plans and providers if they were required to trace the source of any erroneous or

incomplete information transmitted to them.

We would rely on a combination of three other requirements to ensure that protected health information remains as accurate as possible as it travels through the health care system. First, we are proposing that a covered plan or provider that makes an amendment or correction be required to notify any relevant persons, organizations, or other entities of the change or addition. Second, we are proposing that other covered plans or providers that receive such a notification be required to incorporate the necessary amendment or correction. Finally, we are proposing that covered plans or providers require their business partners who receive such notifications to incorporate any necessary amendments or corrections. See discussion in section II.F.4.c.iii. We are soliciting comments whether this approach would effectively ensure that amendments and corrections are communicated appropriately.

iii. *Information available for amendment or correction.*

We are proposing that the right to request amendment or correction extend to all protected health information that would be available for inspection and copying under § 164.514. We would only require covered plans and providers to amend or correct that information maintained in a designated record set but would encourage the development of systems that would accommodate these types of changes for all data collections. For protected health information that is maintained solely by a business partner or that has been materially altered by a business partner, the covered plan or provider would need to make arrangements with the business partner to accommodate any requests.

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

iv. *Duration of the right to request amendment or correction.*

We are proposing that covered plans and providers be required to accommodate requests for amendment or correction for as long as the entity maintains the protected health information. We considered requiring covered plans and providers to accommodate requests for a specific period or defining a specific retention period. We rejected that approach because many laws and professional standards already designate specific retention periods and we did not want to create confusion. In addition, we concluded that individuals should be permitted to request amendments or corrections for as long as the information is maintained by the covered plan or provider. We are soliciting comments on whether we should include a specific duration requirement in this proposed rule.

b. *Grounds for denial of request for amendment or correction.* We are proposing that a covered plan or provider would be permitted to deny a request for amendment or correction if, after a reasonable review, the plan or provider determines that it did not create the information at issue, the information would not be available for inspection and copying under proposed § 164.514, the information is accurate and complete, or if it is erroneous or incomplete, it would not adversely affect the individual.

c. *Procedures for requesting amendment or correction.*

i. *Individual requests for amendment or correction.*

In § 164.516, we are proposing that covered plans and providers be required to have procedures that enable individuals to exercise their rights to request amendment or correction, including a means by which individuals can request amendment or correction of protected health information about them. We considered whether this proposed rule should include detailed procedures governing an individual's request. But as with the procedures for requesting inspection and copying, we are only providing a general requirement and permitting each plan or provider to develop procedures in accordance with its needs. Once the procedures are developed, the plan or provider would document them in accordance with section § 164.520 and include a brief explanation in the notice that is provided to individuals pursuant to section § 164.512.

ii. *Time limits.*

We are proposing that the covered plan or provider would take action on a request for amendment or correction as quickly as the circumstances require, but not later than 60 days following the request. The justification for establishing a time limitation for amendment and correction is virtually identical to that provided for the time limitation for inspection and copying. We concluded that the entity should be provided with some additional flexibility in this context. Depending on the nature of the request, an amendment or correction could require significantly more time than a request for inspection and copying. If a covered plan or provider needed more than 30 days to make a decision, we would encourage, but not require, it to send an acknowledgment of receipt to the individual including an explanation of the reasons for the delay and a date when the individual can expect a final decision.

iii. *Acceptance of a request for amendment or correction.*

If a covered plan or provider accepts an individual's request for amendment or correction, it would be required to make the appropriate amendments or corrections. In making the change, the entity would have to either add the amended or corrected information as a permanent part of the record or mark the challenged entries as amended or corrected entries and, if appropriate, indicate the place in the record where the amended or corrected information is located. Covered plans or providers would not be required to expunge any protected health information, but rather mark it as erroneous or incomplete.

We also propose in § 164.506(e) that entities include a contract requirement that when the covered plan or provider notifies the business partner of an amendment or correction, the business partner must make the necessary amendments or corrections to protected health information in its custody.

In § 164.516(c)(3), we are proposing that, upon accepting an amendment or correction, the covered plan or provider would be required to make reasonable efforts to notify relevant persons, organizations, or other entities of the change or addition. An entity would be required to notify such persons that the individual identifies, or that the covered plan or provider identifies as (1) a recipient of the erroneous or incomplete information, and (2) a person who:

- Has relied upon that information to the detriment of the individual; or
- Is a person who may foreseeably rely on such erroneous or incomplete information to the detriment of the individual.

We are concerned about the potential burden that this notification requirement would impose on covered plans and providers. We do not, however, anticipate that a significant

number of requests would be submitted to any entity and therefore the need for such notifications would be rare. In addition, we determined that because health information can travel so quickly and efficiently in the modern health care system, the need for notification outweighed the potential burden. It is important to note that a reasonableness standard should be applied to the notification process—if the recipient has not relied upon the erroneous or incomplete information to the detriment of the individual or if it is not foreseeable that the recipient will do so, then it would not be reasonable for the covered plan or provider to incur the time and expense of notification. If, however, the incorrect information is reasonably likely to be used to the detriment of the individual, the entity should make every effort to notify the recipients of the information of the changes as quickly as possible.

iv. *Denial of a request for amendment or correction.*

In proposed § 164.516(c)(4), we would require a covered plan or provider to provide the individual with a written statement in plain language of the reason for the denial and permit the individual to file a written statement of disagreement with the decision to deny the request.

The statement prepared by covered plan or provider would be required to explain the basis for the denial. The statement would include a description of how the individual may complain to the covered plan or provider as provided in § 164.518(d). The statement would include the name and number of the contact person within the plan or provider who is responsible for receiving complaints. The statement also would include information regarding filing a complaint with the Secretary pursuant to § 164.522(b)(1), including the mailing address and any forms that may be available. Finally, the statement would explain that the individual has the right to file a written statement of disagreement that would be maintained with the disputed information and the procedure for filing such a statement of disagreement.

If the individual chooses to file a statement of disagreement, then the covered plan or provider must retain a copy of the statement with the protected health information in dispute. The covered plan or provider could require that the statement be a reasonable length, provided that the individual has reasonable opportunity to state the nature of the disagreement and offer his or her version of accurate and complete information. In all subsequent disclosures of the information requested to be amended or corrected, the covered plan or provider would be required to include a copy of its statement of the basis for denial and, if provided by the individual, a copy of his or her statement of disagreement. If the statement submitted by the individual is unreasonably long, the covered plan or provider could include a summary in subsequent disclosures which reasonably explains the basis of the individual's position. The covered plan or provider would also be permitted to provide a rebuttal to the individual's statement of disagreement and include the rebuttal statement in any subsequent disclosures.

We considered requiring the covered plan or provider to provide a mechanism for appealing denials of amendment or correction but concluded that it would be too burdensome. We are soliciting comment on whether the approach we have adopted reasonably balances the burdens on covered plans or providers with the rights of individuals.

v. *Receipt of a notification of amendment or correction.*

If a covered plan or provider receives a notification of erroneous or incomplete protected health information as provided in proposed § 164.516(d), we are proposing that the covered plan or provider or be required to make the necessary amendment or correction to protected health information in its custody that would be available for inspection and copying. This affirmative duty to incorporate amendments and corrections would be necessary to ensure that individuals' protected health information is as accurate and complete as possible as it travels through the health care system.

G. Administrative Requirements (§ 164.518)

[*Please label comments about this section with the subject: ''Introduction to administrative requirements''*]

In § 164.518, we are proposing general administrative requirements for covered entities. We would require all covered entities to designate a privacy official, train members of their workforce regarding privacy requirements, safeguard protected health information, and establish sanctions for members of the workforce who do not abide by the entity's privacy policies and procedures. In addition, we are proposing that covered plans and providers be required to establish a means for individuals to complain to the covered plan or provider if they believe that their privacy rights have been violated. In the discussions of each proposed provision, we provide examples of how different kinds of covered entities could satisfy these requirements.

1. Designation of a Privacy Official (§ 164.518(a))

[*Please label comments about this section with the subject: ''Privacy official''*]

In proposed § 164.518(a)(1), we would require covered entities to designate an employee or other person to serve as the official responsible for the development of policies and procedures for the use and disclosure of protected health information. The designation of an official would focus the responsibility for development of privacy policy.

We considered whether covered entities should be required to designate a single official or an entire board. We concluded that a single official would better serve the purposes of focusing the responsibility and providing accountability within the entity. The implementation of this requirement would depend on the size of the entity. For example, a small physician's practice might designate the office manager as the privacy official, and he or she would assume this as one of his or her broader administrative responsibilities. A large entity might appoint a person whose sole responsibility is privacy policy, and he or she might choose to convene a committee representing several different components of the entity to develop and implement privacy policy.

In proposed § 164.518(a)(2), we would require a covered entity to designate a contact person or office to receive complaints and provide information about the matters covered by the entity's notice. The covered entity could, but would not be required to, designate the designated privacy official as the entity's contact person.

In proposed § 164.512, we would require the covered plan or provider's privacy notice to include the name of a contact person for privacy matters. We would not require that the contact person and the designated privacy official be the same person. This would be left to the discretion of each covered entity.

2. Training (§ 164.518(b))

[*Please label comments about this section with the subject: ''Training''*]

In proposed § 164.518(b), we would require covered entities to provide training on the entities policies and procedures with respect to protected health information. Each entity would be required to provide initial training by the date on which this proposed rule becomes applicable. After that date, each covered entity would have to

provide training to new members of the workforce within a reasonable time period after joining the entity. In addition, we are proposing that when a covered entity makes material changes in its privacy policies or procedures, it would be required to retrain those members of the workforce whose duties are directly affected by the change within a reasonable time of making the change.

The entities would be required to train all members of the workforce (e.g., all employees, volunteers, trainees, and other persons under the direct control of a persons working on behalf of the covered entity on an unpaid basis who are not business partners) who are likely to have contact with protected health information.

Upon completion of the training, the person would be required to sign a statement certifying that he or she received the privacy training and will honor all of the entity's privacy policies and procedures. Entities would determine the most effective means of communicating with their workforce. For example, in a small physician practice, the training requirement could be satisfied by providing each new member of the workforce with a copy of the practice's information policies and requiring members of the workforce to acknowledge that they have reviewed the policies. A large health plan could provide for a training program with live instruction, video presentations or interactive software programs. The small physician practice's solution would not protect the large plan's data, and the plan's solution would be neither economically feasible nor necessary for the small physician practice.

At least once every three years after the initial training, covered entities would be required to have each member of the workforce sign a new statement certifying that he or she will honor all of the entity's privacy policies and procedures. The initial certification would be intended to make members of the workforce aware of their duty to adhere to the entity's policies and procedures. By requiring a recertification every three years, they would be reminded of this duty.

We considered several different options for recertification. We considered proposing that members of the workforce be required to recertify every six months, but concluded that such a requirement would be too burdensome. We considered proposing that recertification be required annually consistent with the recommendations of The American Health Information Management Association (Brandt, Mary D., Release and Disclosure: Guidelines Regarding Maintenance and Disclosure of Health Information, 1997). We concluded that annual recertification could also impose a significant burden on covered entities.

We also considered requiring that the covered entity provide ''refresher'' training every three years in addition to the recertification. We concluded that our goals could be achieved by only requiring recertification once every three years, and retraining in the event of material changes in policy. We are soliciting comment on this approach.

3. Safeguards (§ 164.518(c))

[*Please label comments about this section with the subject: ''Safeguards''*]

In proposed § 164.518(c), we would require covered entities to put in place administrative, technical, and physical safeguards to protect against any reasonably anticipated threats or hazards to the privacy of the information, and unauthorized uses or disclosures of the information. We proposed similar requirements for certain electronic information in the Notice of Proposed Rulemaking entitled the Security and Electronic Signature Standards (HCFA–0049–P), which can be found at 63 FR 43241. We are proposing parallel and consistent requirements for safeguarding the privacy of protected health information.

a. *Verification procedures.* As noted in section II.E. above, for many permitted disclosures the covered entity would be responding to a request for disclosure of protected health information. For most categories of permitted disclosures, when the request for disclosure of protected health information is from a person with whom the covered entity does not routinely do business, we would require the covered entity to verify the identity of the requestor. In addition, for certain categories of disclosures, covered entities would also be required to verify the requestor's legal authority to make the request.

Under § 164.514, a covered entity would be required to give individuals access to protected health information about them (under most circumstances). The covered entity would also be required to take reasonable steps to verify the identity of the individual making the request for access. We do not propose to mandate particular identification requirements (*e.g.*, drivers licence, photo ID, etc), but rather would leave this to the discretion of the covered entity.

Covered entities would be required to verify both the identity of persons requesting protected health information and their authority for requesting such information when the request is from a person with whom the covered entity does not routinely do business and the disclosure would be permitted by the following subsections of § 164.510: under § 164.510(b) for public health, under § 164.510(c) for oversight, under § 164.510(e) to coroners and medical examiners, under § 164.510(f) for law enforcement, under § 164.510(g) for governmental health data systems, under § 164.510(m) for special classes, and for disclosures required by other laws under § 164.510(n). Covered entities would be required to verify the identity of the requester by examination of reasonable evidence, such as a written statement of identity on agency letterhead, an identification badge, or similar proof of official status. Similarly, covered entities would be required to verify the legal authority supporting the request by examination of reasonable evidence, such as a written request provided on agency letterhead that describes the legal authority for requesting the release. Unless § 164.510 explicitly requires written evidence of legal process or other authority before a disclosure may be made, a public official's proof of identity and the official's oral statement that the request is authorized by law would be presumed to constitute the required reasonable evidence of legal authority. Where § 164.510 does require written evidence of legal process or authority, only the required written evidence will suffice.

We considered specifying the type of documentation or proof that would be acceptable, but decided that the burden of such specific regulatory requirements on covered entities would be unnecessary. Therefore, we propose only a general requirement for reasonable verification of identity and legal authority.

In § 164.522, we would require disclosure to the Secretary for purposes of enforcing this regulation. When a covered entity is asked by the Secretary to disclose protected health information for compliance purposes, the covered entity should verify the same information that it would verify for any other law enforcement or oversight request for disclosure.

In some circumstances a person or entity acting on behalf of a government agency may make a request for disclosure of protected health information under these subsections. For example, public health agencies may contract with a nonprofit agency to collect and analyze certain data. In such cases the covered entity would be required to verify the requestor's identity and authority through

examination of reasonable documentation that the requestor is acting on behalf of the government agency. Reasonable evidence would include a written request provided on agency letterhead that describes the legal authority for requesting the release and states that the person or entity is acting under the agency's authority, or other documentation, including a contract, a memorandum of understanding, or purchase order that confirms that the requestor is acting on behalf of the government agency.

For disclosures permitted under § 164.510(k) for emergency circumstances and under § 164.510(l) to next-of-kin, legal authority for the request would not be an issue. Therefore covered entities would only be required to verify the identity of the person requesting the disclosure. Where protected health information is requested by next-of-kin, covered entities would be required to make reasonable verbal attempts to establish the identity of the person making the request. Written proof would not be required. Covered entities could rely on prior acquaintance with the next-of-kin; verbal verification of identity would not be required at each encounter. Where protected health information is requested in an emergency, the covered entity would similarly not be required to demand written proof that the person requesting the protected health information is legally authorized. Reasonable reliance on verbal representations would be appropriate in such situations.

When another person is acting as the individual through power of attorney or other legal authority, covered entities would also be required to make reasonable attempts to ascertain that the person making the request has the necessary legal authority or relationship in order to make the disclosure. For example, a health care provider could require a copy of a power of attorney, or could ask questions to determine that an adult acting for a young child has the requisite relationship to the child.

Most disclosures under § 164.510(i) are routine transactions with banking and other financial institutions. As noted above, for routine transactions there would be no verification requirements. However, should such financial institution make a special request for information in addition to the information routinely provided for payment purposes (*e.g.*, pursuant to a fraud or similar investigation), the covered entity would be required to obtain reasonable evidence of the identity of the person requesting the information.

The conditions for disclosures for judicial and administrative proceedings and research are discussed in § 164.510 (d) and § 164.510(j), respectively. Conditions for permitted disclosures under § 164.510(h) for facility directories include no verification requirements.

b. *Whistleblowers.* In Section § 164.518(c)(4), we would address the issue of disclosures by employees or others of protected health information in whistleblower cases. We would clarify that under the proposed rule, a covered entity would not be held in violation because a member of their workforce or a person associated with a business partner of the covered entity discloses protected health information that such person believes is evidence of a civil or criminal violation, and the disclosure is: (1) Made to relevant oversight agencies and law enforcement or (2) made to an attorney to allow the attorney to determine whether a violation of criminal or civil law has occurred or to assess the remedies or actions at law that may be available to the person disclosing the information.

Allegations of civil and criminal wrongdoing come from a variety of sources. Sometimes an individual not otherwise involved in law enforcement uncovers evidence of wrongdoing, and wishes to bring that evidence to the attention of appropriate authorities. Persons with access to protected health information sometimes discover evidence of billing fraud or similar violations; important evidence of unlawful activities may be available to employees of covered entities, such as billing clerks or nurses.

Some whistleblower activities can be accomplished without individually identifiable health information. There are, however, instances in which only identifiable information will suffice to demonstrate that an allegation of wrongdoing merits the investment of legal or investigatory resources. A billing clerk who suspects that a hospital has engaged in fraudulent billing practices may need to use billing records for a set of specific cases to demonstrate the basis of his suspicion to an oversight agency.

The persons who find such evidence are likely to be employees of the suspect entity. Congress and the states have recognized the importance of whistleblowing activities by acting to protect whistleblowers from retaliation. Federal statutes that include protections for whistleblowers who contact appropriate authorities include the Clear Air Act, the Federal Water Pollution Control Act, the Toxic Substances Control Act, and the Safe Drinking Water Act. Congress also passed the Whistleblower Protection Act, to protect federal employees who complain about improper personnel practices at federal agencies. At least eleven states have passed whistleblower protection laws that protect both private and public employees who provide evidence of wrongdoing to the appropriate authorities, and many more states have laws that provide such protections only for public employees.

The qui tam provisions of the Federal False Claims Act go further, and provide a mechanism for the individual to prosecute a case against a person who has allegedly defrauded the government. Like traditional whistleblower actions, qui tam actions were created by the Congress to further the public interest in effective government. Qui tam suits are an important way that individuals can protect the public interest, by investing their own time and resources to help reduce fraud. And, also like whistleblower actions, the individual may need protected health information to convince an attorney that a viable qui tam case exists.

We would note that this section would not apply to information requested by oversight agencies, law enforcement officials, or attorneys, even prior to initiation of an investigation or law suit. It would apply only to a disclosure initiated by a member of an entity's workforce or a person associated with one of its business partners.

We are concerned that a person, in the guise of ''whistleblowing,'' might, maliciously or otherwise, disclose protected health information without any actual basis to believe that there has been a violation of the law. We are concerned, however, with adding qualifying language that may restrict such disclosures and, therefore, impede the pursuit of law violators. We seek comments regarding whether this provision should include any limitations (*e.g.*, a requirement that only the minimum amount of information necessary for these purposes can be disclosed).

4. Internal Complaint Process (§ 164.518(d))

In proposed § 164.518(d), we would require covered plans and providers to have some mechanism for receiving complaints from individuals regarding the covered plan's or provider's compliance with the requirements of this proposed rule. The covered plan or provider would be required to accept complaints about any aspect of their practices regarding protected health information. For example, individuals would be able to file a complaint when

they believe that protected health information relating to them has been used or disclosed improperly, that an employee of the plan or provider has improperly handled the information, that they have wrongfully been denied access to or opportunity to amend the information, or that the entity's notice does not accurately reflect its information practices. We would not require that the entity develop a formal appeals mechanism, nor that ''due process'' or any similar standard be applied. We would not require that covered entities respond in any particular manner or time frame. We are proposing two basic requirements for the complaint process. First, the covered plan or provider would be required to identify a contact person or office in the notice of information practices for receiving complaints. This person or office could either be responsible for handling the complaints or could put the individual in touch with the appropriate person within the entity to handle the particular complaint. See proposed § 164.512. This person could, but would not have to be, the entity's privacy official. See § 164.518(a)(2). Second, the covered plan or provider would be required to maintain a record of the complaints that are filed and a brief explanation of the resolution, if any.

Covered plans and providers could implement this requirement through a variety of mechanisms based on their size and capabilities. For example, a small practice could assign a clerk to log in written and/or verbal complaints as they are received, and assign one physician to review all complaints monthly, address the individual situations and make changes to policies or procedures as appropriate. Results of the physician's review of individual complaints then could be logged by the clerk. A larger provider or health plan could choose to implement a formal appeals process with standardized time frames for response.

We considered requiring covered plans and providers to provide a formal internal appeal mechanism, but rejected that option as too costly and burdensome for some entities. We also considered eliminating this requirement entirely, but rejected that option because a complaint process would give covered plans or providers a way to learn about potential problems with privacy policies or practices, or training issues. We also hope that providing an avenue for covered plans or providers to address complaints would lead to increased consumer satisfaction. We believe this approach strikes a reasonable balance between allowing covered plans or providers flexibility and accomplishing the goal of promoting attention to improvement in privacy practices. If an individual and a covered plan or provider are able to resolve the individual's complaint, there may be no need for the individual to file a complaint with the Secretary under proposed § 164.522(b). However, an individual has the right to file a complaint with the Secretary at any time. An individual may file a complaint with the Secretary before, during, after, or concurrent with filing a compliant with the covered plan or provider or without filing a complaint with the covered plan or provider.

We are considering whether modifications of these complaint procedures for intelligence community agencies may be necessary to address the handling of classified information and solicit comment on the issue.

5. Sanctions (§ 164.518(e))

[*Please label comments about this section with the subject: ''Sanctions''*]

In proposed § 164.518(e), we would require all covered entities to develop and apply when appropriate sanctions for failure to comply with policies or procedures of the covered entity or with the requirements of this proposed rule. All members of the workforce who have regular contact with protected health information should be subject to sanctions, as would the entity's business partners. Covered entities would be required to develop and impose sanctions appropriate to the nature of the issue. The type of sanction applied would vary depending on factors such as the severity of the violation, whether the violation was intentional or unintentional, and whether the violation indicates a pattern or practice of improper use or disclosure of protected health information. Sanctions could range from a warning to termination.

We considered specifying particular sanctions for particular kinds of violations of privacy policy, but rejected this approach for several reasons. First, the appropriate sanction will vary with the entity's particular policies. Because we cannot anticipate every kind of privacy policy in advance, we cannot predict the response that would be appropriate when that policy is violated. In addition, it is important to allow covered entities to develop the sanctions policies appropriate to their business and operations.

6. Duty To Mitigate (§ 164.518(f))

[*Please label comments about this section with the subject: ''Duty to mitigate''*]

We propose that covered entities be required to have procedures for mitigating, to the extent practicable, any deleterious effect of a use or disclosure of protected health information by their members of their workforce or business partners.

With respect to business partners, we also propose that covered entities have an affirmative duty to take reasonable steps in response to breaches of contract terms. For example, a covered entity that becomes aware that a business partner has improperly disclosed protected health information could require that business partner to take steps to retrieve the disclosed information. The covered entity also could require that business partner to adopt new practices to better assure that protected health information is appropriately handled. Covered entities generally would not be required to monitor the activities of their business partners, but would be required to take steps to address problems of which they become aware, and, where the breach is serious or repeated, would also be required to monitor the business partner's performance to ensure that the wrongful behavior has been remedied. For example, the covered entity could require the business partner to submit reports or subject itself to audits to demonstrate compliance with the contract terms required by this rule. Termination of the arrangement would be required only if it becomes clear that a business partner cannot be relied upon to maintain the privacy of protected health information provided to it.

We expect that sanctions would be more formally described and consistently carried out in larger, more sophisticated entities. Smaller, less sophisticated entities would be given more latitude and flexibility. For such smaller entities and less sophisticated entities, we would not expect a prescribed sanctions policy, but would expect that actions be taken if repeated instances of violations occur.

H. Development and Documentation of Policies and Procedures (§ 164.520)

[*Please label comments about this section with the subject: ''Policies and procedures''*]

In proposed § 164.520, we would require covered entities to develop and document their policies and procedures for implementing the requirements of this rule. This requirement is intended as a tool to facilitate covered entities' efforts to develop appropriate policies to implement this rule, to ensure that the members of its workforce and business partners understand and carry out expected privacy practices, and to assist

covered entities in developing a notice of information practices.

The scale of the policies developed should be consistent with the size of the covered entity. For example, a smaller employer could develop policies restricting access to health plan information to one designated employee, empowering that employee to deny release of the information to corporate executives and managers unless required for health plan administration. Larger employers could have policies that include using contractors for any function that requires access to protected health information or requiring all reports they receive for plan administration to be de-identified unless individual authorization is obtained.

Clearly, implementation of these requirements would differ significantly based on the size, capabilities and activities of each covered entity. A solo practitioner's documentation of her policies and procedures could provide relatively straightforward statements, such as:

> This practice does not use or disclose any protected health information that is not authorized or permitted under the federal privacy regulation and therefore does not request any authorized disclosures from patients. Staff R.N. reviews all individually authorized requests for disclosures to ensure they contain all required elements and reviews the copied information to ensure only authorized information is released in response. Information requests that would require extensive redaction will be denied.

Larger entities with many functions and business relationships and who are subject to multi-state reporting and record-keeping requirements would need to develop and document more extensive policies. A health plan would need to describe all activities that would be considered health care operations and identify the use and disclosure requirements of each activity. A health plan may determine that underwriting department employees must provide a written request, approved by a team leader, to access any identifiable claims information; that such requests must be retained and reviewed every quarter for appropriateness; and the underwriting department must destroy such information after use for an approved activity. We urge professional associations to develop model policies, procedures and documentation for their members of all sizes.

We are proposing general guidelines for covered entities to develop and document their own policies and procedures. We considered a more uniform, prescriptive approach but concluded that a single approach would be neither effective in safeguarding protected health information nor appropriate given the vast differences among covered entities in size, business practices and level of sophistication. It is important that each covered entity's internal policies and procedures for implementing the requirements of this regulation are tailored to the nature and number of its business arrangements, the size of its patient population, its physical plant and computer system, the size and characteristics of its workforce, whether it has one or many locations, and similar factors. The internal policies and procedures appropriate for a clearinghouse would not be appropriate for a physician practice; the internal policies and procedures appropriate for a large, multi-state health plan would not be appropriate for a smaller, local health plan.

After evaluating the requirements of federal, State, or other applicable laws, covered entities should develop policies and procedures that are appropriate for their size, type, structure, and business arrangements. Once a covered plan or provider has developed and documented all of the policies and procedures as required in this section, it would have compiled all of the information needed to develop the notice of information practices required in § 164.512. The notice is intended to include a clear and concise summary of many of the policies and procedures discussed in this section. Further, if an individual has any questions about the entity's privacy policies that are not addressed by the notice, a representative of the entity can easily refer to the documented policies and procedures for additional information.

Before making a material change in a policy or procedure, the covered entity would, in most instances, be required to make the appropriate changes to the documentation required by this section before implementing the change. In addition, covered plans and providers would be required to revise the notice of information practices in advance. Where the covered entity determines that a compelling reason exists to take an action that is inconsistent with its documentation or notice before making the necessary changes, it may take such action if it documents the reasons supporting the action and makes the necessary changes within 30 days of taking such action.

In an attempt to ensure that large entities develop coordinated and comprehensive policies and procedures as required by this section, we considered proposing that entities with annual receipts greater than $5 million [5] be required to have a privacy board review and approve the documentation of policies and procedures. As originally conceived, the privacy board would only serve to review research protocols as described in § 164.510(j). We believe that such a board could also serve as ''privacy experts'' for the covered entity and could review the entity's documented policies and procedures. In this capacity, the overriding objective of the board would be to foster development of up-to-date, individualized policies that enable the organization to protect health information without unnecessarily interfering with the treatment and payment functions or business needs. This type of review is particularly important for large entities who would have to coordinate policies and procedures among a large staff, but smaller organizations would be encouraged, but not required, to take a similar approach (*i.e.*, have a widely representative group participate in the development and/or review of the organization's internal privacy policies and the documentation thereof). We solicit comment on this proposal.

We also considered requiring the covered entity to make its documentation available to persons outside the entity upon request. We rejected this approach because covered entities should not be required to share their operating procedures with the public, or with their competitors.

We recognize that the documentation requirement in this proposed rule would impose some paperwork burden on covered plans and providers. However, we believe that it is necessary to ensure that covered plans and providers establish privacy policies procedures in advance of any requests for disclosure, authorization, or subject access. It is also necessary to ensure that covered entities and members of their workforce have a clear understanding of the permissible uses and disclosures of protected health information and their duty to protect the privacy of such information under specific circumstances.

1. Uses and Disclosures of Protected Health Information

We propose that covered entities be required to develop and document policies and procedures for how protected health information would be used and disclosed by the entity and its

[5] The Small Business Administration defines small businesses in the health care field as those generating less than $5 million annually. Small businesses represent approximately 85% of health care entities.

business partners. The documentation would include policies to ensure the entity is in compliance with the requirements for use and disclosure pursuant to an individual's authorization. This would also include documentation of how the covered entity would comply with individual's revocation of an authorization, as provided in proposed § 164.508(e). For example, upon receipt of a revocation, the entity may need to take steps to notify each business partner that is responsible for using or disclosing protected health information on behalf of the covered entity based on the individual's authorization. Because the entity is ultimately responsible for the protected health information, it may want written confirmation from the business partner that it received notice of the revocation.

The covered entity would be required to include policies and procedures necessary to address disclosures required by applicable law. For example, the covered entity may want to include a list of the relevant reporting requirements such as those for abuse, neglect and communicable disease and its policies and procedures for complying with each requirement.

It would also include policies and procedures for uses and disclosures without the individual's authorization, including uses and disclosures for treatment, payment and health care operations under § 164.506(a)(1)(i). The documentation should address all of the legally permissible uses and disclosures that the covered entity is reasonably likely to make and should clearly specify the policy of the entity with respect to each. For example, all covered plans and providers face a reasonable likelihood of a request for disclosure from a health oversight agency, so every covered plan and provider should develop and document policies and procedures for responding to such requests. However, a provider that only treats adults would not need to specify a policy with respect to state laws that authorize disclosure relating to measles in young children. In this latter case, the provider knows that he or she is not reasonably likely to make such a disclosure and therefore, could wait until he or she is presented with such a request before developing the necessary policies and procedures.

The documentation would include the entity's policies and procedure for complying with the requirements of proposed § 164.506(e) for disclosing protected health information to business partners, including policies and procedures for monitoring the business partners, mitigating harm, and imposing sanctions where appropriate.

It would address the policies and procedures for implementation of the minimum necessary requirement as provided in proposed § 164.506(b). It would also include policies and procedures addressing the creation of de-identified information pursuant to § 164.506(d). For example, a plan could have a policy that requires employees to remove identifiers from protected health information for all internal cost, quality, or performance evaluations. The plan would document this policy and the procedures for removing the identifiers.

2. Individual Requests for Restricting Uses and Disclosures

We propose to require covered health care providers to document how they would implement an individual's request to restrict uses and disclosures. Under proposed § 164.506(c)(1)(iii), a covered entity need not agree to such restrictions. This section of the documentation would describe who (if anyone) in the covered entity is permitted to agree to such restrictions, and if such restrictions were accepted, how they would be implemented. For example, a provider may require that once an individual has requested a limitation on a use or disclosure, the affected information is stamped, marked or kept in a separate file. The provider could also have a policy of never agreeing to requests for such restrictions.

3. Notice of Information Practices

We propose to require covered plans and providers to document their policies and procedures for complying with the requirement in § 164.512 to develop, make available or disseminate, and amend their notices of information practices. This documentation would address, at a minimum, who is responsible for developing and updating the notice, who would serve as the ''contact'' person on the notice, how the notice would be disseminated to individuals, and how to respond to inquiries regarding information practices.

4. Inspection and Copying

We propose to require covered plans and providers to document policies and procedures to address how they would receive and comply with individual requests for inspection, and copying, in compliance with § 164.514 of this proposed rule. Policies and procedures should address, at a minimum, a listing of the designated record sets to which access will be provided, any fees to be charged, and the reasons (if any) that the entity would deny a request for inspection and copying.

5. Amendment or Correction

We propose to require covered plans and providers to develop and document policies and procedures to address how they would receive and comply with individual requests for amendment or correction of their records, in compliance with § 164.516 of this proposed rule. Policies and procedures should include the process for determining whether a request for amendment or correction should be granted, the process to follow if a request is denied, and how the entity would notify other entities, including business partners, if the request is accepted. For example, if a covered entity accepts an individual's request for an amendment or correction, the entity could document specific procedures regarding how to make the appropriate additions or notations to the original information. Without such documentation, members of the workforce could accidentally expunge or remove the incorrect information.

6. Accounting for Disclosures

We propose to require covered entities to develop and document their policies and procedures for complying with the requirement in § 164.515 to provide on request an accounting for disclosures for purposes other than treatment, payment or health care operations. In order to respond to requests for accounting within a reasonable period of time, the entity would need to have a system for accounting in place well in advance of any potential requests. The entity would need to evaluate its record keeping system and determine how best to build in the capacity to respond to such a request. For example, if the entity chooses to keep a regular log of disclosures, it would have to begin keeping such logs routinely. If instead the entity chooses to rely on a record keeping system to reconstruct an accounting, it should develop appropriate procedures for members of the workforce to follow when faced with an individual's request.

7. Administrative Requirements

We propose to require covered entities to document their policies and procedures for complying with the applicable administrative requirements in proposed § 164.518. This would include designation of the privacy official required by § 164.518(a) including a description of his or her responsibilities; a description of how the entity would comply with the

training and certification requirements for members of its workforce under § 164.518(b); a description of the covered entity's safeguards required by § 164.518(c); a description of how the covered plan or provider would meet the requirements of § 164.518(d) to receive individual's complaints; a description of how the covered entity would meet the requirements for sanctioning members of its workforce under § 164.518(e); and a description of how the covered entity would take steps to mitigate any deleterious effect of a use or disclosure of protected health information as required by § 164.518(f).

The documentation would also address how access to protected health information is regulated by the entity, including safeguards, including the procedures that would be required by proposed § 164.518. For covered entities that are part of a larger organization that is not a covered entity (*e.g.*, an on-site clinic at a university or the group health plan component of an employer), we would require such entities to develop and document policies and procedures that ensure that protected health information does not flow outside the health care component of the organization in violation of this proposed rule. For example, a school-based health clinic should have policies and procedures to prevent treatment information from crossing over into the school's record system.

Many disclosures would require verification of the identity of the person making the request, and sometimes also verification of the legal authority behind the request. The documentation required by this section would include a description of the entity's verification policies (*e.g.*, what proof would be acceptable), and who would be responsible for ensuring that the necessary verification has occurred before the information is disclosed.

8. Record Keeping Requirements

We propose record keeping requirements related to several provisions. In addition to the documentation of policies and procedures described above, we would require covered entities, as applicable, to: document restrictions on uses and disclosures agreed to pursuant to § 164.506(c); maintain copies of authorization forms and signed authorizations (§ 164.508) and contracts used with business partners (§ 164.506(e)); maintain notices of information practices developed under § 164.512; maintain written statements of denials of requests for inspection and copying pursuant to § 164.514; maintain any response made to a request from an individual for amendment or correction of information, either in the form of the correction or amendment or the statement of the reason for denial and, if supplied, the individual's statement of disagreement, for as long as the protected health information is maintained (§ 164.516); maintain signed certifications by members of the workforce required by § 164.518(b); and, maintain a record of any complaints received (§ 164.518(d)). Unless otherwise addressed in this proposal, covered entities would be required to retain these documents for six years, which is the statute of limitations period for the civil penalties. We note that additional records or compliance reports may be required by the Secretary for enforcement of this rule. (§ 164.522(d)(1)).

I. Relationship to Other Laws

1. Relationship to State Laws

[*Please label comments about this section with the subject: ''Relationship to State laws''*]

Congress addressed the issue of preemption of State law explicitly in the statute, in section 1178 of the Act. Consonant with the underlying statutory purpose to simplify the financial and administrative transactions associated with the provision of health care, the new section 1178(a)(1) sets out a ''general rule'' that State law provisions that are contrary to the provisions or requirements of part C of title XI or the standards or implementation specifications adopted or established thereunder are preempted by the federal requirements. The statute provides three exceptions to this general rule: (1) For State laws which the Secretary determines are necessary to prevent fraud and abuse, ensure appropriate State regulation of insurance and health plans, for State reporting on health care delivery, and other purposes; (2) for State laws which address controlled substances; and (3) for State laws relating to the privacy of individually identifiable health information which, as provided for by the related provision of section 264(c)(2), are contrary to and more stringent than the federal requirements. Section 1178 also carves out, in sections 1178(b) and 1178(c), certain areas of State authority which are not limited or invalidated by the provisions of part C of title XI; these areas relate to public health and State regulation of health plans.

Section 264 of HIPAA contains a related preemption provision. Section 264(c)(2) is, as discussed above, an exception to the ''general rule'' that the federal standards and requirements preempt contrary State law. Section 264(c)(2) provides, instead, that contrary State laws that relate to the privacy of individually identifiable health information will not be preempted by the federal requirements, if they are ''more stringent'' than those requirements. This policy, under which the federal privacy protections act as a floor, but not a ceiling on, privacy protections, is consistent with the Secretary's Recommendations.

Aside from the cross-reference to section 264(c)(2) in section 1178(a)(2)(B), several provisions of section 1178 relate to the proposed privacy standards. These include the general preemption rule of section 1178(a)(1), the carve-out for public health and related reporting under section 1178(b), and the carve-out for reporting and access to records for the regulation of health plans by States under section 1178(c). Other terms that occur in section 264(c)(2) also appear in section 1178: The underlying test for preemption—whether a State law is ''contrary'' to the federal standards, requirements or implementation specifications—appears throughout section 1178(a), while the issue of what is a ''State law'' for preemption purposes applies throughout section 1178. In light of these factors, it seems logical to develop a regulatory framework that addresses the various issues raised by section 1178, not just those parts of it implicated by section 264(c)(2). Accordingly, the rules proposed below propose regulatory provisions covering these issues as part of the general provisions in proposed part 160, with sections made specifically applicable to the proposed privacy standard where appropriate.

a. *The ''general rule'' of preemption of State law.* Section 1178(a)(1) provides the following ''general rule'' for the preemption of State law:

> Except as provided in paragraph (2), a provision or requirement under this part (part C of title XI), or a standard or implementation specification adopted or established under sections 1172 through 1174, shall supersede any contrary provision of State law, including a provision of State law that requires medical or health plan records (including billing information) to be maintained or transmitted in written rather than electronic form.

As we read this provision, the provisions and requirements of part C of title XI, along with the standards and implementation specifications adopted thereunder, do not supplant State law, except to the extent such State law is ''contrary'' to the federal statutory or regulatory scheme. Moreover, the provisions and requirements of part C of

title XI, along with the standards and implementation specifications adopted thereunder, do not preempt contrary State law where one of the exceptions provided for by section 1178(a)(2) applies or the law in question lies within the scope of the carve-outs made by sections 1178(b) and (c). Thus, States may continue to regulate in the area covered by part C of title XI and the regulations and implementation specifications adopted or established thereunder, except to the extent States adopt laws that are contrary to the federal statutory and regulatory scheme, and even those contrary State laws may continue to be enforceable, if they come within the statutory exceptions or carve-outs.

We note, however, that many of the Administrative Simplifications regulations will have preemptive effect. The structure of many of the regulations, particularly those addressing the various administrative transactions, is to prescribe the use of a particular form or format for the transaction in question. Where the prescribed form or format is used, covered entities are required to accept the transaction. A State may well not be able to require additional requirements for such transactions consistent with the federally prescribed form or format.

b. *Exceptions for State laws the Secretary determines necessary for certain purposes.* Section 1178(a)(2) lists several exceptions to the general preemption rule of section 1178(a)(1). The first set of exceptions are those listed at sections 1178(a)(2)(A)(i) and 1178(a)(2)(A)(ii). These exceptions are for provisions of State law which the Secretary determines are necessary: (1) To prevent fraud and abuse; (2) to ensure appropriate State regulation of insurance and health plans; (3) for State reporting on health care delivery or costs; (4) for other purposes; or (5) which address controlled substances.

Proposed § 160.203(a) below provides for determinations under these statutory provisions. The criteria at proposed § 160.203(a) follow the statute. As is more fully discussed below, however, two of the terms used in this section of the proposed rules are defined terms: ''contrary'' and ''State law.'' The process for making such determinations is discussed below.

c. *Exceptions for State laws relating to the privacy of individually identifiable health information.* The third exception to the ''general rule'' that the federal requirements, standards, and implementation specifications preempt contrary State law concerns State laws relating to the privacy of individually identifiable health information. Section 1178(a)(2)(B) provides that a State law is excepted from this general rule, which, ''subject to section 264(c)(2) of the Health Insurance Portability and Accountability Act of 1996, relates to the privacy of individually identifiable health information.'' Section 264(c)(2) of HIPAA provides that the HIPAA privacy regulation, which is proposed in the accompanying proposed subpart B of proposed part 160, will not supersede ''a contrary provision of State law, if the provision of State law imposes requirements, standards, or implementation specifications that are more stringent than the requirements, standards, or implementation specifications imposed'' under the regulation at proposed subpart E of proposed part 164.

It is recognized that States generally have laws that relate to the privacy of individually identifiable health information. These laws continue to be enforceable, unless they are contrary to part C of title XI or the standards, requirements, or implementation specifications adopted or established pursuant to the proposed subpart x. Under section 264(c)(2), not all contrary provisions of State privacy laws are preempted; rather, the law provides that contrary provisions that are also ''more stringent'' than the federal regulatory requirements or implementation specifications will continue to be enforceable.

d. *Definitions.* There are a number of ambiguities in sections 1178(a)(2)(B) and 264(c)(2) of HIPAA. Clarifying the statute through the regulations will generally provide substantially more guidance to the regulated entities and the public as to which requirements, standards, and implementation specifications apply. For these reasons, the rules propose below to interpret several ambiguous statutory terms by regulation.

There are five definitional questions that arise in considering whether or not a State law is preempted under section 264(c)(2): (1) What is a ''provision'' of State law? (2) What is a ''State law''? (3) What kind of State law, under section 1178(a)(2)(B), ''relates to the privacy of individually identifiable health information?'' (4) When is a provision of State law at issue ''contrary'' to the analogous provision of the federal regulations? (5) When is a provision of State law ''more stringent than'' the analogous provision of the federal regulations? We discuss these questions and our proposed regulatory answers below.

i. *What is a ''provision'' of State law?*

The initial question that arises in the preemption analysis is, what does one compare? The statute directs this analysis by requiring the comparison of a ''provision of State law [that] imposes requirements, standards, or implementations specifications'' with ''the requirements, standards, or implementation specifications imposed under'' the federal regulation. The statute thus appears to contemplate that what will be compared are the State and federal requirements that are analogous, i.e., that address the same subject matter. Accordingly, a dictionary-type definition of the term ''provision'' does not seem appropriate, as the contours of a given ''provision'' will be largely defined by the contours of the specific ''requirement[], standard[], or implementation specification'' at issue.

What does one do when there is a State provision and no comparable or analogous federal provision, or the converse is the case? The short answer would seem to be that, since there is nothing to compare, there cannot be an issue of a ''contrary'' requirement, and so the preemption issue is not presented. Rather, the stand-alone requirement—be it State or federal—is effective. There may, however, be situations in which there is a federal requirement with no directly analogous State requirement, but where several State requirements in combination would seem to be contrary in effect to the federal requirement. This situation usually will be addressed through the tests for ''contrary,'' discussed below.

At this juncture, it is difficult to frame options for dealing with this issue, because it is not clear that more of a structure is needed than the statute already provides. Rather, we solicit comment on how the term ''provision'' might be best defined for the purpose of the preemption analysis under the statute, along with examples of possible problems in making the comparison between a provision of State law and the federal regulations.

ii. *What is a ''State law''?*

It is unclear what the term ''provision of State law'' in sections 1178 and 264(c) means. The question is whether the provision in question must, in order to be considered to have preemptive effect, be legislatively enacted or whether administratively adopted or judicially decided State requirements must also be considered. Congress explicitly addressed the same issue in a different part of HIPAA, section 102. Section 102 enacted section 2723 of the Public Health Service Act, which is a preemption provision that applies to issuers of health insurance to ERISA plans. Section 2723 contains in subsection (d)(1) the following definition of ''State law'': ''The term

''State law'' includes all laws, decisions, rules, regulations, or other State action having the effect of law, of any State. A law of the United States applicable only to the District of Columbia shall be treated as a State law rather than a law of the United States.

By contrast, Congress provided no definition of the term ''State law'' in section 264. This omission suggests two policy options. One is to adopt the above definition, as a reasonable definition of the term and as an indication of what Congress probably intended in the preemption context (the policy embodied in section 2723 is analogous to that embodied in section 264(c)(2), in the sense that the State laws that are not preempted are ones that provide protections to individuals that go above and beyond the federal requirements). The other option is to argue by negative implication that, since Congress could have but did not enact the above definition in connection with sections 264 and 1178, it intended that a different definition be used, and that the most reasonable alternative is to limit the State laws to be considered to those that have been legislatively enacted.

The Department does not consider the latter option to be a realistic one. It is legally questionable and is also likely to be extremely confusing and unworkable as a practical matter, as it will be difficult to divorce State ''laws'' from implementing administrative regulations or decisions or from judicial decisions. Also, much State ''privacy law''—e.g., the law concerning the physician/patient privilege—is not found in statutes, but is rather in State common law. Finally, since health care providers and others are bound by State regulations and decisions, they would most likely find a policy that drew a line based on where a legal requirement originated very confusing and unhelpful. As a result, we conclude that the language in section 102 represents a legally supportable approach that is, for practical reasons, a realistic option, and it is accordingly proposed in proposed § 160.202 below.

iii. *What is a law that ''relates to the privacy of individually identifiable health information''?*

The meaning of the term ''relate to'' has been extensively adjudicated in a somewhat similar context, the issue of the preemption of State laws by ERISA. Section 514(a) of ERISA (29 U.S.C. 1144(a)) provides that ERISA ''shall supersede any and all State laws insofar as they may now or hereafter *relate to* any employee benefit plan.'' (Emphasis added.) The U.S. Supreme Court alone has decided 17 ERISA preemption cases, and there are numerous lower court cases. The term also has been interpreted in other contexts. Thus, there would seem to be several options for defining the term ''relates to'': (1) By using the criteria developed by the Supreme Court as they evolve, (2) by using the criteria developed by the Supreme Court, but on a static basis, and (3) based on the legislative history, by setting federal criteria.

The first option would be based on the definition adopted in an early ERISA case, *Shaw* v. *Delta Airlines, Inc.*, 463 U.S. 85 (1983), as it continues to evolve. In *Shaw*, a unanimous Supreme Court adopted a very broad reading of the term, holding that a law ''relates to'' an employee benefit plan ''if it has a connection with or reference to'' such a plan. Later cases have developed a more particularized and complex definition of this general definition. The Supreme Court has also applied the *Shaw* definition outside of the ERISA context. In *Morales* v. *Trans World Airlines*, 504 U.S. 374 (1992), the Court defined the term ''relating to'' in the Airline Deregulation Act by using the definition of the term ''relates to'' developed under the ERISA cases above. While this option would appear to be a supportable reading of the statutory term, tying the agency interpretation to an evolving court interpretation will make it more difficult to make judgments, and particular judgments may change as the underlying court interpretations change.

The second option we considered would ''freeze'' the definition of ''relates to'' as the Court has currently defined it. This option also is a supportable reading of the statutory term, but is less of a moving target than the prior option. The complexity of the underlying court definition presents problems.

The option selected and reflected in the rules proposed below grows out of the movement in recent years of the Supreme Court away from the literal, textual approach of *Shaw* and related cases to an analysis that looks more at the purposes and effects of the preemption statute in question. In *New York State Conference of Blue Cross* v. *Travelers Insurance Co.*, 514 U.S. 645 (1995), the Court held that the proper inquiry in determining whether the State law in question related to an employee benefit plan was to look to the objectives of the (ERISA) statute as a guide to the scope of the State law that Congress understood would survive. The Court drew a similar line in *Morales*, concluding that State actions that affected airline rates, routes, or services in ''too tenuous, remote, or peripheral a manner'' would not be preempted. 504 U.S. at 384. The Court drew a conceptually consistent line with respect to the question of the *effect* of a State law in *English* v. *General Electric Co.*, 496 U.S. 72, 84 (1990); see also, *Gade* v. *National Solid Wastes Management Ass'n.*, 505 U.S. 88 (1992). The Court held that deciding which State laws were preempted by the OSH Act required also looking at the effect of the State law in question, and that those which regulated occupational safety and health in a ''clear, direct, and substantial way'' would be preempted. These cases suggest an approach that looks to the legislative history of HIPAA and seeks to determine what kinds of State laws Congress meant, in this area, to leave intact and also seeks to apply more of a ''rule of reason'' in deciding which State laws ''relate to'' privacy and which do not.

The legislative history of HIPAA offers some insight into the meaning of the term ''relates to.'' The House Report (House Rep. No. 496, 104th Cong., 2d Sess., at 103) states that—

> The intent of this section is to ensure that State privacy laws that are more stringent than the requirements and standards contained in the bill are not superseded.

Based on this legislative history, one could argue that the ''State laws'' covered by the ''relates to'' clause are simply those that are specifically or explicitly designed to regulate the privacy of personal health information, and not ones that might have the incidental effect of doing so. Thus, the option selected below appears to be consistent with the Court's approach in *Travelers*, and, together with the ''effect'' test, seems to be closer to how the Court is analyzing preemption issues. It makes sense on a common sense basis as well, and appears, from the little legislative history available, to be what Congress intended in this context.

iv. *When is a provision of State law ''contrary'' to the analogous federal requirement?*

The statute uses the same language in both section 1178(a)(1) and section 264(c)(2) to delineate the general precondition for preemption: the provision of State law must be ''contrary'' to the relevant federal requirement, standard, or implementation specification; the term ''contrary,'' however, is not defined. It should be noted that this issue (the meaning of the term ''contrary'') does not arise solely in the context of the proposed privacy standard. The term ''contrary'' appears throughout section 1178(a) and is a precondition for any preemption analysis done under that section.

The definition set out at proposed § 160.202 embodies the tests that the courts have developed to analyze what is known as ''conflict preemption.'' In this analysis, the courts will consider a provision of State law to be in conflict with a provision of federal law where it would be impossible for a private party to comply with both State and federal requirements or where the provision of State law ''stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress.'' This latter test has been further defined as, where the State law in question ''interferes with the methods by which the federal statute was designed to reach (its) goal.'' *International Paper Co.* v. *Ouellette,* 479 U.S. 481, 494 (1987). In *Gade,* the Supreme Court applied this latter test to preempt an Illinois law and regulations that imposed additional, non-conflicting conditions on employers, holding that the additional conditions conflicted with the underlying congressional purpose to have one set of requirements apply. This test, then, is particularly relevant with respect to the other HIPAA regulations, where Congress clearly intended uniform standards to apply nationwide.

The Department is of the view that this definition should be workable and is probably what Congress intended in using the term—as a shorthand reference to the case law. We considered a broader definition (''inconsistent with''), but rejected it on the grounds that it would have less legal support and would be no easier to apply than the statutory term ''contrary'' itself.

v. *What is the meaning of ''more stringent''?*

The issue of when a provision of State law is ''more stringent'' than the comparable ''requirements, standards, or implementation specifications'' of the HIPAA privacy regulation is not an easy one. In general, it seems reasonable to assume that ''more stringent'' means ''providing greater privacy protection'' but, such an interpretation leads to somewhat different applications, depending on the context. For example, a State law that provided for fewer and more limited disclosures than the HIPAA privacy regulation would be ''more stringent.'' At the same time, a State law that provides for more and/or greater penalties for wrongful disclosures than does the HIPAA privacy regulation would also be ''more stringent.'' Thus, in the former case, ''more stringent'' means less or fewer, while in the latter case, ''more stringent'' means more or greater. In addition, some situations are more difficult to characterize. For example, if the HIPAA privacy regulation requires disclosure to the individual on request and a State law prohibits disclosure in the circumstance in question, which law is ''more stringent'' or ''provides more privacy protection'?

A continuum of regulatory options is available. At one end of the continuum is the minimalist approach of not interpreting the term ''more stringent'' further or spelling out only a general interpretation, such as the ''provides more privacy protection'' standard, and leaving the specific applications to later case-by-case determinations. At the other end of the continuum is the approach of spelling out in the regulation a number of different applications, to create a very specific analytic framework for future determinations. We propose below the latter approach for several reasons: specific criteria will simplify the determination process for agency officials, as some determinations will be already covered by the regulation, while others will be obvious; specific criteria will also provide guidance for determinations where issue of ''stringency'' is not obvious; courts will be more likely to give deference to agency determinations, leading to greater uniformity and consistency of expectation; and the public, regulated entities, and States will have more notice as to what the determinations are likely to be.

The specific criteria proposed at proposed § 160.202 are extrapolated from the principles of the fair information practices that underlie and inform these proposed rules and the Secretary's Recommendations. For example, limiting disclosure of personal health information obviously protects privacy; thus, under the criteria proposed below, the law providing for less disclosure is considered to be ''more stringent.'' Similarly, as the access of an individual to his or her protected health information is considered to be central to enabling the individual to protect such information, the criteria proposed below treat a law granting greater rights of access as ''more stringent.'' We recognize that many State laws require patients to authorize or consent to disclosures of their health information for treatment and/or payment purposes. We consider individual authorization generally to be more protective of privacy interests than the lack of such authorization, so such State requirements would generally stand, under the definition proposed below.

However, we would interpret a State law relating to individual authorization to be preempted if the law requires, or would permit a provider or health plan to require, as a condition of treatment or payment for health care, an individual to authorize uses or disclosures for purposes other than treatment, payment and health care operations, and if such authorization would override restrictions or limitations in this regulation relating to the uses and disclosures for purposes other than treatment, payment and health care operations. For example, if a State law permitted or required a provider to obtain an individual authorization for disclosure as a condition of treatment, and further permitted the provider to include in the authorization disclosures for research or for commercial purposes, the State law would be preempted with respect to the compelled authorization for research or commercial purposes. At the same time, if a State law required a provider to obtain an individual authorization for disclosure as a condition of treatment, and further required the provider to include an authorization for the provider to disclosure data to a State data reporting agency, such a law would not be preempted, because State laws that require such data reporting are saved from preemption under section § 1178(c) of the statute.

In addition, to the extent that a State consent law does not contain other consent or authorization requirements that parallel or are stricter than the applicable federal requirements, those detailed federal requirements would also continue to apply. We solicit comment in particular on how these proposed criteria would be likely to operate with respect to particular State privacy laws.

e. *The process for making administrative determinations regarding the preemption of State health information privacy laws.* Because States generally have laws that relate to the privacy of individually identifiable health information, there may be conflicts between provisions of various State laws and the federal requirements. Where such conflicts appear to exist, questions may arise from the regulated entities or from the public concerning which requirements apply. It is possible that such questions may also arise in the context of the Secretary's enforcement of the civil monetary penalty provisions of section 1176. The Secretary accordingly proposes to adopt the following process for responding to such comments and making the determinations necessary to carry out her responsibilities under section 1176.

The rules proposed below would establish two related processes: one for making the determinations called for by

section 1178(a)(2)(A) of the Act and the other for issuing advisory opinions regarding whether a provision of State law would come within the exception provided for by section 1178(a)(2)(B).

i. *Determinations under section 1178(a)(2)(A).*

The rules proposed below should not usually implicate section 1178(a)(2)(A), which provides that a State law will not be preempted where the Secretary determines it is necessary for one or more of five specific purposes: (1) To prevent fraud and abuse; (2) to ensure appropriate State regulation of insurance and health plans; (3) for State reporting on health care delivery or costs; (4) for other purposes; or (5) which address controlled substances. The process for implementing this statutory provision is proposed here, because the issue of how such preemption issues will be handled has been raised in prior HIPAA rulemakings and needs to be addressed, and, as explained above, the statutory provision itself is fairly intertwined (in terms of the specific terms used), with the preemption provisions of the statute that relate to privacy.

The process proposed below for determinations by the Secretary would permit States to request an exception to the general rule of preemption. The decision to limit, at least as an initial matter, the right to request such determinations to States was made for several reasons. First, States are obviously most directly concerned by preemption, in that it is State legislative, judicial, or executive action that the federal requirements supersede. Principles of comity dictate that States be given the opportunity to make the case that their laws should not be superseded. Second, States are in the best position to address the issue of how their laws operate and what their intent is, both of which are relevant to the determination to be made. Third, we need to control the process as an initial matter, so that the Secretary is not overwhelmed by requests. Fourth, where particular federal requirements will have a major impact on providers, plans, or clearinghouses within a particular State, we assume that they will be able to work with their State governments to raise the issue with the Secretary; the discussion process that such negotiations should entail should help crystallize the legal and other issues for the Secretary and, hence, result in better determinations. We emphasize that HHS may well revisit this issue, once it has gained some experience with the proposed process.

Proposed § 160.204(a)(1) sets out a number of requirements for requests for determinations. In general, the purpose of these requirements is to provide as complete a statement as possible of the relevant information as an initial matter, to minimize the time needed for the Secretarial determination.

The remaining requirements of proposed § 160.204(a) generally are designed to set out an orderly process and effect of the determinations. Of particular note is proposed § 160.204(a)(5), which provides that such determinations apply only to transactions that are wholly intrastate. We recognize that in today's economy, many, perhaps most, transactions will be interstate, so that the effect of a positive determination could be minimal under this provision. Nonetheless, we think that there is no practical alternative to the proposed policy. We do not see how it would be practical to split up transactions that involved more than one State, when one State's law was preempted and the other's was not. We do not see why the non-preempted law should govern the transaction, to the extent it involved an entity in a State whose law was preempted. Quite aside from the sovereignty issues such a result would raise, such a result would be very confusing for the health care industry and others working with it and thus inconsistent with the underlying goal of administrative simplification. Rather, such a situation would seem to be a classic case for application of federal standards, and proposed § 160.204(a)(5) would accordingly provide for this.

ii. *Advisory opinions under section 1178(a)(2)(B).*

The rules proposed below lay out a similar process for advisory opinions under section 1178(a)(2)(B). That section of the statute provides that, subject to the requirements of section 264(c)(2) (the provision of HIPAA that establishes the ''more stringent'' preemption test), State laws that ''relate to the privacy of individually identifiable health information'' are excepted from the general rule that the HIPAA standards, requirements, and implementation specifications preempt contrary State law.

Unlike section 1178(a)(2)(A), section 1178(a)(2)(B) does not provide for the making of a determination by the Secretary. Nonetheless, it is clear that the Secretary may make judgments about the legal effect of particular State privacy laws in making compliance and enforcement decisions. It is also foreseeable that the Secretary will be asked to take a position on whether particular State privacy laws are preempted or not. We have concluded that the best way of addressing these concerns is to provide a mechanism by which the Secretary can issue advisory opinions, so that the public may be informed about preemption judgments the Secretary has made. See proposed § 160.204(b).

The process proposed below for requesting advisory opinions is limited to States, for the reasons described in the preceding section. The requirements for requests for advisory opinions are similar to the requirements for determinations in proposed § 160.204(a), but are tailored to the different statutory requirements of sections 1178(a)(2)(A) and 264(c)(2). As with proposed § 164.204(a), the process proposed below would provide for publication of advisory opinions issued by the Secretary on an annual basis, to ensure that the public is informed of the decisions made in this area.

f. *Carve-out for State public health laws.* Section 1178(b) provides that ''Nothing in this part shall be construed to invalidate or limit the authority, power, or procedures established under any law providing for the reporting of disease or injury, child abuse, birth, or death, public health surveillance, or public health investigation or intervention.'' This section appears to carve out an area over which the States have traditionally exercised oversight and authority—the collection of vital statistics, the enforcement of laws regarding child abuse and neglect, and the conduct of public health surveillance, investigation, and intervention. State laws in these areas may involve reporting of individually identifiable health information to State or local authorities. Section 1178(b) indicates that existing or future State laws in these areas are enforceable, notwithstanding any privacy requirements adopted pursuant to section 264(c). In addition, covered entities should not be inhibited from complying with requests authorized by State law for release of information by public health authorities for the stated purposes.

It should be noted that the limitation of section 1178(b) applies to the ''authority, power, or procedures established under any law.'' Public health laws often convey broad general authorities for the designated agency to protect public health, including enforcement powers, and these State authorities and powers would remain enforceable. Further, section 1178(b) also covers ''procedures'' authorized by law; we read this language as including State administrative regulations and guidelines.

The proposed rules propose to address these concerns by treating the

disclosures covered by section 1178(b) as allowable disclosures for public health activities under proposed § 164.510(b). Thus, those disclosures permitted under proposed § 164.510(b) are intended to be, with respect to disclosures authorized by State law, at least as broad as section 1178(b). This means that disclosures that are authorized by State law but which do not come within the scope of proposed § 164.510(b) are considered to fall outside of the limitation of section 1178(b). In addition, since similar activities and information gathering are conducted by the federal government, disclosures to public health authorities authorized by federal law would be permitted disclosures under this proposed rule and applicable federal law will govern the use and re-disclosure of the information.

g. *Carve-out for State laws relating to oversight of health plans.* Section 1178(c) provides that nothing in part C of title XI limits the ability of States to require health plans ''to report, or to provide access to, information for management audits, financial audits, program monitoring and evaluation, facility licensure or certification, or individual licensure or certification.'' This section thus also carves out an area in which the States have traditionally regulated health care as an area which the statute intends to leave in place. State laws requiring the reporting of or access to information of the type covered by section 1178(c) will in certain cases involve the reporting of, or access to, individually identifiable health information. Accordingly, provision has been made for such reporting and access by making such reporting and access permitted disclosures and uses under this proposed rule. See proposed § 164.510(c).

2. Relationship to Other Federal Laws

[*Please label comments about this section with the subject: ''Relationship to other federal laws''*]

The rules proposed below also would affect various federal programs, some of which may have requirements that are, or appear to be, inconsistent with the requirements proposed below. Such federal programs include those programs that are operated directly by the federal government, such as the health benefit programs for federal employees or the health programs for military personnel. They also include a wide variety of health services or benefit programs in which health services or benefits are provided by the private sector or by State or local government, but which are governed by various federal laws. Examples of the latter types of programs would be the Medicare and Medicaid programs, the health plans governed by the Employee Retirement Income Security Act of 1974, 29 U.S.C. 1001, *et seq.* (ERISA), the various clinical services programs funded by federal grants, and substance abuse treatment programs.

Some of the above programs are explicitly covered by HIPAA. Section 1171 of the Act defines the term ''health plan'' to include the following federally conducted, regulated, or funded programs: group plans under ERISA which either have 50 or more participants or are administered by an entity other than the employer who established and maintains the plan; federally qualified health maintenance organizations; Medicare; Medicaid; Medicare supplemental policies; the health care program for active military personnel; the health care program for veterans; the Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); the Indian health service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, *et seq.;* and the Federal Employees Health Benefits Program. There also are many other federally conducted, regulated, or funded programs in which individually identifiable health information is created or maintained, but which do not come within the statutory definition of ''health plan.'' While these latter types of federally conducted, regulated, or assisted programs are not explicitly covered by part C of title XI in the same way that the programs listed in the statutory definition of ''health plan'' are covered, the statute may nonetheless apply to transactions and other activities conducted under such programs. This is likely to be the case where the federal entity or federally regulated or funded entity provides health services; the requirements of part c are likely to apply to such an entity as a ''health care provider.'' Thus, the issue of how different federal requirements apply is likely to arise in numerous contexts.

When two federal statutes appear to conflict, the courts generally engage in what is called an ''implied repeal'' analysis. The first step in such an analysis is to look for some way in which to reconcile the apparently conflicting requirements. Only if the conflicting provisions cannot be reconciled do courts reach the second step of the analysis, in which they look to see whether the later statute repealed the prior statute (to the extent of the conflict) by implication. In making such a determination, the courts look to the later statute and its legislative history, to see if there is evidence as to whether Congress intended to leave the prior statute in place or whether it intended the later statute to supersede the prior statute, to the extent of the conflict between the two. It is not a foregone conclusion that a later statute will repeal inconsistent provisions of a prior statute. Rather, there are cases in which the courts have held prior, more specific statutes not to be impliedly repealed by later, more general statutes.

As noted above, the section 1171 of the Act explicitly makes certain federal programs subject to the standards and implementation specifications promulgated by the Secretary, while entities carrying out others are implicitly covered by the scope of the term ''health care provider.'' The legislative history of the statute is silent with respect to how these requirements were to operate in the federal sector vis-à-vis these and other federal programs with potentially conflicting requirements. Congress is presumed to have been aware that various federal programs that the privacy and other standards would reach would be governed by other federal requirements, so the silence of the legislative history and the limited reach of the statute would seem to be significant. On the other hand, Congress' express inclusion of certain federal programs in the statute also has significance, as it constitutes an express Congressional statement that the HIPAA standards and implementation specifications apply to these programs. In light of the absence of relevant legislative history, we do not consider this Congressional statement strong enough to support a conclusion of implied repeal, where the conflict is one between the HIPAA regulatory standards and implementation specifications and another federal statute. However, it seems strong enough to support an inference that, with respect to these programs, the HIPAA standards and implementation specifications establish the federal policy in the case of a conflict at the regulatory level.

Thus, the first principle that applies where both the HIPAA standards and implementation specifications and the requirements of another federal program apply is that we must seek to reconcile and accommodate any apparently conflicting federal requirements. Two conclusions flow from this principle. First, where one federal statute or regulation permits an activity that another federal statute or regulation requires, and both statutes apply to the entity in question, there is no conflict, because it is possible to comply with both sets of federal requirements.

Second, where one federal statute or regulation permits, but does not require, an activity that another federal statute or regulation prohibits, there is again no conflict, because it is possible to comply with both sets of federal requirements. In each case, the entity has lost some discretion that it would otherwise have had under the more permissive set of requirements, but in neither case has it been required to do something that is illegal under either federal program.

There will, however, also be cases where the privacy or other Administrative Simplification standards and implementation specifications cannot be reconciled with the requirements of another federal program. In such a case the issue of implied repeal is presented. As suggested above, we think that where the conflict is between the privacy or other Administrative simplification regulations and another federal statute, the regulatory requirements would give way, because there is insufficient evidence to support a finding that part C of title XI is intended to repeal other federal laws. For example, if other law prohibits the dissemination of classified or other sensitive information, this rule's requirements for granting individuals' right to copy their own records would give way. Where the conflict is between the Administrative Simplification regulatory requirements and other federal regulatory requirements that are discretionary (not mandated by the other federal law), we think that there is also insufficient evidence to support a finding of implied repeal of the latter regulatory requirements, where the other federal program at issue is not one specifically addressed in section 1171. However, where the other federal program at issue is one of the ones which Congress explicitly intended to have the Administrative Simplification standards and implementation specifications apply to, by including them in the definition of ''health plan'' in section 1171, we think that there is evidence that the Administrative Simplification standards and implementation specifications should prevail over contrary exercises of discretion under those programs.

We considered whether the preemption provision of section 264(c)(2) of Public Law 104–191, discussed in the preceding section, would give effect to State laws that would otherwise be preempted by federal law. For example, we considered whether section 264(c)(2) could be read to make the Medicare program subject to State laws relating to information disclosures that are more stringent than the requirements proposed in this rule, where such laws are presently preempted by the Medicare statute. We also considered whether section 264(c)(2) could be read to apply such State laws to procedures and activities of federal agencies, such as administrative subpoenas and summons, that are prescribed under the authority of federal law. In general, we do not think that section 264(c)(2) would work to apply State law provisions to federal programs or activities with respect to which the State law provisions do not presently apply. Rather, the effect of section 264(c)(2) is to give preemptive effect to State laws that would otherwise be in effect, to the extent they conflict with and are more stringent than the requirements promulgated under the Administrative Simplification authority of HIPAA. Thus, we do not believe that it is the intent of section 264(c)(2) to give an effect to State law that it would not otherwise have in the absence of section 264(c)(2).

We explore some ramifications of these conclusions with respect to specific federal programs below. We note that the summaries below do not identify all possible conflicts or overlaps of the proposed rules with other federal requirements; rather, we have attempted to explain the general nature of the relationship of the different federal programs. We would anticipate issuing more detailed guidance in the future, when the final privacy policies are adopted, and the extent of conflict or overlap can be ascertained. We also invite comment with respect to issues raised by other federal programs.

a. *The Privacy Act.* The Privacy Act of 1974, 5 U.S.C. 552a, is not preempted or amended by part C of title XI. The Privacy Act applies to all federal agencies, and to certain federal contractors who operate Privacy Act protected systems of records on behalf of federal agencies. It does not, however, apply to non-federal entities that are reached by part C. While the proposed rules are applicable to federal and non-federal entities, they are not intended to create any conflict with Privacy Act requirements. In any situation where compliance with the proposed rules would lead a federal entity to a result contrary to the Privacy Act, the Privacy Act controls. In sections of the proposed rules which might otherwise create the appearance of a conflict with Privacy Act requirements, entities subject to the Privacy Act are directed to continue to comply with Privacy Act requirements.

Because the Privacy Act gives federal agencies the authority to promulgate agency-specific implementing regulations, and because the Privacy Act also allows agencies to publish routine uses that have the status of exceptions to the Privacy Act's general rule prohibiting disclosure of Privacy Act protected information to third parties, the issue of possible conflicts between the proposed Administrative Simplification rules and existing Privacy Act rules and routine uses must be addressed. Where the federal program at issue is one of the ones that Congress explicitly intended to have the Administrative Simplification standards and implementation specifications apply to, by including them in the definition of ''health plan'' in section 1171, we think that there is evidence that the Administrative Simplification standards and implementation specifications should prevail over contrary exercises of discretion under those programs. That is, to the extent that a routine use is truly discretionary to an agency which is also a covered entity under section 1172(a), the agency would not have discretion to ignore the Administrative Simplification regulations. It is possible, however, that in some cases there might be underlying federal statutes that call for disclosure of certain types of information, and routine uses could be promulgated as the only way to implement those statutes and still comply with the Privacy Act. If this were to happen or be the case, the routine use should prevail.

b. *The Substance Abuse Confidentiality regulations.* Regulations that are codified at 42 CFR part 2 establish confidentiality requirements for the patient records of substance abuse ''programs'' that are ''federally assisted.'' Substance abuse programs are specialized programs or personnel that provide alcohol and drug abuse treatment, diagnosis, or referral for treatment. 42 CFR 2.11. The term ''federally assisted'' is broadly defined, and includes federal tax exempt status and Medicare certification, among other criteria. 42 CFR 2.12(b). Such programs may not disclose patient identifying information without the written consent of the patient, unless the information is needed to respond to a medical emergency, or such information is disclosed for purposes of research, audit, or evaluation. Disclosures may not be made in response to a subpoena; rather, a court order is required in order for a disclosure of covered records to be lawfully made. Limited disclosures may also be made by such programs to State or local officials under a State law requiring reporting of incidents of suspected child abuse and neglect and

to law enforcement officials regarding a patient's crime on program premises or against program personnel or a threat to commit such a crime. 42 CFR 2.12. Unlike the rules proposed below, the confidentiality protections continue indefinitely after death, although part 2 would permit disclosure of identifying information relating to the cause of death under laws relating to the collection of vital statistics or permitting inquiry into cause of death.

It seems likely that most, if not all, programs covered by the part 2 regulations will also be covered, as health care providers, by the rules proposed below. As can be seen from the above summary, the part 2 regulations would not permit many disclosures that would be permitted under proposed § 164.510 below, such as many disclosures for law enforcement, directory information, governmental health data systems, and judicial and other purposes. In addition, the general permissive disclosure for treatment or payment purposes at proposed § 164.506 below would be inconsistent with the more restrictive requirements at part 2. In such situations, providers (or others) subject to both sets of requirements could not make disclosures prohibited by part 2, even if the same disclosures would be permitted under the rules proposed below.

There are also a number of requirements of the part 2 regulations that parallel the requirements proposed below. For example, the minimum necessary rule, where applicable, would parallel a similar requirement at 42 CFR 2.13(a). Similarly, the notice requirements of part 2, at 42 CFR 2.22 parallel the notice requirements proposed below, although the notice required below would be more detailed and cover more issues. The preemptive effect on State law should be the same under both part 2 and section 264(c)(2). The requirements for disclosures for research proposed below are likewise similar to those in part 2. In such cases, health care providers would have to comply with the more extensive or detailed requirements, but there should be no direct conflict.

Many other provisions of the proposed rules, however, simply have no counterpart in part 2. For example, the part 2 regulations do not require programs to maintain an accounting of uses and disclosures, nor do they provide for a right to request amendment or correction of patient information. Similarly, the part 2 regulations contain no prohibition on conditioning treatment or payment on provision of an individual authorization for disclosure. In such situations, health care providers would be bound by both sets of requirements.

c. *ERISA.* ERISA was enacted in 1974 to regulate pension and welfare employee benefit plans that are established by private sector employers, unions, or both, to provide benefits to their workers and dependents. An employee welfare benefit plan includes plans that provide ''through the purchase of insurance or otherwise * * * medical, surgical, or hospital care or benefits, or benefits in the event of sickness, accident, disability, (or) death.'' 29 U.S.C. 1002(1). In 1996, Public Law 104–191 amended ERISA to require portability, nondiscrimination, and renewability of health benefits provided by group health plans and group health insurance issuers. Numerous, although not all, ERISA plans are covered under the rules proposed below as ''health plans.''

As noted above, section 514(a) of ERISA, 29 U.S.C. 1144(a), preempts all State laws that ''relate to'' any employee benefit plan. However, section 514(b) of ERISA, 29 U.S.C. 1144(b)(2)(A), expressly saves from preemption State laws which regulate insurance. Section of ERISA, 29 U.S.C. 1144(b)(2)(B), provides that an ERISA plan is deemed not to be an insurer for the purpose of regulating the plan under the State insurance laws. Thus, under the deemer clause, States may not treat ERISA plans as insurers subject to direct regulation by State law. Finally, section 514(d) of ERISA, 29 U.S.C. 1144(d), provides that ERISA does not ''alter, amend, modify, invalidate, impair, or supersede any law of the United States.''

We considered whether the preemption provision of section 264(c)(2) of Public Law 104–191, discussed in the preceding section, would give effect to State laws that would otherwise be preempted by section 514(a) of ERISA. Our reading of the statutes together is that the effect of section 264(c)(2) is simply to leave in place State privacy protections that would otherwise apply and which are more stringent than the federal privacy protections. In the case of ERISA plans, however, if those laws are preempted by section 514(a), they would not otherwise apply. We do not think that it is the intent of section 264(c)(2) to give an effect to State law that it would not otherwise have in the absence of section 264(c)(2). Thus, we would not view the preemption provisions below as applying to State laws otherwise preempted by section 514(a) of ERISA.

Many plans covered by the rules proposed below are also subject to ERISA requirements. To date our discussions and consultations have not uncovered any particular ERISA requirements that would conflict with the rules proposed below. However, we invite comment, particularly in the form of specific identification of statutory or regulatory provisions, of requirements under ERISA that would appear to conflict with provisions of the rules proposed below.

d. *Other federally funded health programs.* There are a number of authorities under the Public Health Service Act and other legislation that contain explicit confidentiality requirements either in the enabling legislation or in the implementing regulations. Many of these are so general that there would appear to be no problem of inconsistency, in that nothing in the legislation or regulations would appear to restrict the assisted provider's discretion to comply with the requirements proposed below. There are, however, several authorities under which either the requirements of the enabling legislation or of the program regulations would impose requirements that would differ from the rules proposed below. We have identified several as presenting potential issues in this regard. First, regulations applicable to the substance abuse block grant program funded under section 1943(b) of the Public Health Service Act require compliance with 42 CFR part 2, and thus raise the issues identified in section 2 above. Second, there are a number of federal programs which, either by statute or by regulation, restrict the disclosure of patient information to, with minor exceptions, disclosures ''required by law.'' See, for example, the program of projects for prevention and control of sexually transmitted diseases funded under section 318(e)(5) of the Public Health Service Act (42 CFR 51b.404); the regulations implementing the community health center program funded under section 330 of the Public Health Service Act (42 CFR 51c.110); the regulations implementing the program of grants for family planning services under title X of the Public Health Service Act (42 CFR 59.15); the regulations implementing the program of grants for black lung clinics funded under 30 U.S.C. 437(a) (42 CFR 55a.104); the regulations implementing the program of maternal and child health projects funded under section 501 of the Act (42 CFR 51a.6); the regulations implementing the program of medical examinations of coal miners (42 CFR 37.80(a)). These legal requirements would restrict the grantees or other entities under the programs

involved from making many of the disclosures that proposed § 164.510 would permit. In some cases, permissive disclosures for treatment, payment or health care operations would also be limited. Since proposed § 164.510 is merely permissive, there would not be a conflict between the program requirements, as it would be possible to comply with both. However, it should be recognized that entities subject to both sets of requirements would not have the total range of discretion that the rules proposed below would suggest.

J. Compliance and Enforcement (§ 164.522)

1. Compliance

[*Please label written comments about this section with the subject: ''Compliance.''*]

The rules proposed below at § 164.522 would establish several requirements designed to enable the Secretary to monitor and seek to ensure compliance with the provisions of this subpart. The general philosophy of this section is to provide a cooperative approach to obtaining compliance, including use of technical assistance and informal means to resolve disputes. However, in recognition of the fact that it would not always be possible to achieve compliance through cooperation, the section also would provide the Secretary with tools for carrying out her statutory mandate to achieve compliance.

a. *Principles for achieving compliance.* Proposed § 164.522(a) would establish the principle that the Secretary will seek the cooperation of covered entities in obtaining compliance. Section 164.522(a)(2) provides that the Secretary could provide technical assistance to covered entities to help them come into compliance with this subpart. It is clearly in the interests of both the covered entities and the individuals they serve to minimize the costs of compliance with the privacy standards. To the extent that the Department could facilitate this by providing technical assistance, it would endeavor to do so.

b. *Individual complaints and compliance reviews.* We are proposing in § 164.522(b) that individuals have the right to file a complaint with the Secretary if they believe that a covered plan or provider has failed to comply with the requirements of this subpart. Because individuals would have received notice, pursuant to proposed § 164.512, of the uses and disclosures that the entity could make and of the entity's privacy practices, they would have a basis for making a realistic judgment as to when a particular action or omission would be improper. The notice would also inform individuals how they could find out how to file such complaints. We thus consider the proposed complaint right to be one that could realistically be exercised by individuals, given the regulatory structure proposed.

We are concerned about the burden that handling the potential volume of such complaints would create for this Department, but we recognize that such a complaint mechanism would provide helpful information about the privacy practices of covered plans or providers and could serve to identify particularly troublesome compliance problems on an early basis.

The procedures proposed in this section are modeled on those used by the Department's Office for Civil Rights, although they would be adapted to reflect the requirements of this subpart. We would require complainants to identify the entities and describe the acts or omissions alleged to be out of compliance and would require individuals to file such complaints within 180 days of those acts or omissions. We have tried to keep the requirements for filing complaints as minimal as possible, to facilitate use of this right. The Secretary would also attempt to keep the identity of complainants confidential, if possible. However, we recognize that it could be necessary to disclose the identity of complainants in order to investigate the substance of their complaints, and the rules proposed below would permit such disclosures.

The Secretary could promulgate alternative procedures for complaints based on agency-specific concerns. For example, to protect classified information, we may promulgate rules that would allow an intelligence community agency to create a separate body within that agency to receive complaints.

The Secretary would try to resolve complaints on an informal basis wherever possible. Where a resolution could not be reached, the Secretary could make a formal finding of noncompliance. However, resolution could occur, and an agreement reached with the covered entity, even after a finding that a violation occurred. The Secretary could use the finding as a basis to initiate an action under section 1176 of the Act or to refer the matter to the Department of Justice for prosecution under section 1177 of the Act. It should be recognized that the decision to initiate an action under either section of the law would be a discretionary one, and proposed § 164.522 would not require such prosecutorial action to be taken. Proposed § 164.522(e)(1)(ii) would, however, permit the use of findings made in connection with a complaint, group of complaints, or compliance review to be acted on in this fashion.

The rules proposed below also would provide that the Secretary would inform both the covered plan or provider and the complainant, whenever a decision was made on a complaint.

We are proposing in § 164.522(c) that the Secretary could conduct compliance reviews to determine whether covered entities are in compliance. A compliance review could be based on information indicating a possible violation of this subpart even though a formal complaint has not been filed. As is the case with a complaint investigation, a compliance review may examine the policies, practices or procedures of a covered entity and may result in voluntary compliance or in a violation or no violation finding.

c. *Responsibilities of covered entities.* Proposed § 164.522(d) establishes certain obligations for covered entities that would be necessary to enable the Secretary to carry out her statutory role to determine their compliance with these requirements. Proposed § 164.522(d)(1) would require covered entities to maintain records as directed. Proposed § 164.522(d)(2) would require them to participate as required in compliance reviews. Proposed § 164.522(d)(3) would affirmatively establish their obligation to provide information to the Secretary upon demand. Finally, paragraph (d)(4) would prohibit intimidating, discriminatory or other retaliatory actions by a covered entity against a person who files a complaint with the Secretary; testifies, assists or participates in any manner in an investigation, compliance review, proceeding, or hearing under this Act; or opposes any act or practice made unlawful by this subpart. This language is modeled after the Americans with Disabilities Act and title VII of the Civil Rights Act of 1964. Prohibitions against retaliation are also common throughout Department programs. The experience of the federal government in enforcing civil rights and other laws has been that voluntary compliance with and effective enforcement of such laws depend in large part on the initiative of persons opposed to illegal practices. If retaliation for opposing practices that a person reasonably believes are unlawful were permitted to go unremedied, it would have a chilling effect upon the willingness of persons to speak out and

to participate in administrative processes under this subpart.

Opposition to practices of covered entities refers to a person's communication of his or her good faith belief that a covered entity's activities violate this subpart. Opposition includes, but is not limited to, filing a complaint with the covered entity under § 164.518(d) and making a disclosure as a whistleblower under § 164.518(c)(4). This provision would not protect a person whose manner of opposition is so unreasonable that it interferes with the covered entities' legitimate activities. This provision would cover such situations such as where an employee of a physician is fired in retaliation for confronting the doctor regarding her practice of illegally disclosing individuals' records or where a health plan drops coverage after an enrollee argues to the plan that he has a right to access to his records.

We recognize that under these requirements the covered entity would be disclosing protected health information to representatives of the Department when such information is relevant to a compliance investigation or assessment. We recognize that this would create a mandatory disclosure of protected health information and that such a requirement carries significant privacy concerns. Those concerns must, however, be weighed against the need to obtain compliance by entities with the privacy standards, and to protect against future improper uses and disclosures of protected health information. The proposed rule accordingly attempts to strike a balance between these interests, providing that the Department would not disclose such information, except as may be necessary to enable the Secretary to ascertain compliance with this subpart or in enforcement proceedings or as otherwise required by law.

2. Enforcement

[*Please label written comments about this section with the subject: ''Enforcement.''*]

Congress established a two-pronged approach to enforcement of all of the requirements established under part C of title XI of the Act. First, section 1176 grants the Secretary the authority to impose civil monetary penalties against those covered entities which fail to comply with the requirements established under part C. These penalties are to be imposed according to the procedures established for imposition of civil monetary penalties in section 1128A of the Act. Second, section 1177 establishes criminal penalties for certain wrongful disclosures of individually identifiable health information.

The selection of the civil monetary penalty process at section 1128A of the Act as the enforcement mechanism for the Administrative Simplification standards and requirements indicates the type of process Congress believes is appropriate for civil enforcement of those standards and requirements. The Secretary's Recommendations call for a privacy right of action to permit individuals to enforce their privacy rights. However, the HIPAA does not provide a private right of action, so the Secretary lacks the authority to provide for such a remedy. Accordingly, we would provide that individuals could file complaints with the Secretary and the Secretary could then, when appropriate, investigate. The Secretary may also conduct compliance reviews. See proposed § 164.522(b) and (c).

Under section 1177(a), the offense of ''wrongful disclosure'' is a disclosure that violates the standards or requirements established under part C. These would include any disclosures not otherwise permitted under the privacy standards or the parallel security standards.

As we noted in the Notices of Proposed Rulemaking for the other Administrative Simplification regulations, we will propose regulations in the future to establish these procedures. Because such procedures will not constitute ''standards'' within the meaning of part C, they would not be subject to the delay in effective date provisions that apply to the various Administrative Simplification regulations.

III. Small Business Assistance

This rule is significant because it establishes for the first time a federally required regime of information practices in the medical industry. The length, and at times complexity, of the preamble discussion may impress small businesses as creating overly burdensome and costly requirements. We believe, however, that several features of the rule, combined with initiatives by the Department and professional associations, will make the rule easily administrable for the vast majority of small businesses.

First, a significant portion of the rule addresses the topic of signed individual authorization for disclosure of health information—the information that the authorization would include and when such an authorization would be required. Importantly, no patient written authorization would be required when information is disclosed for purposes of treatment and payment and health care operations, or when disclosure is mandated by law. In other words, doctors who disclose patient health information only to other doctors for treatment purposes, or to insurance companies to process payment, or for operational purposes can continue to do so without any change in current practices under this proposal. Only those covered entities who disclose health information to marketers, reporters, private investigators, researchers, and others for purposes unrelated to treatment, payment, and health care operations are required to get the written consent of the patient in accordance with this rule.

Second, the Department plans to engage in outreach and education programs to ease the implementation of this rule for small businesses. Already, this rule provides model forms for getting patient authorization and provides an example of a notice of information practices (another requirement in the rule, described further below). We also expect that professional associations will develop forms tailored to specific groups' needs. The Department pledges to work with professional associations to provide the greatest possible guidance to small businesses covered by this rule.

Third, in implementing this rule, we will apply the principle of ''scalability,'' so that a particular entity's characteristics—including its size, type of business, and information practices—would be relevant to how that entity adopts procedures to comply with this rule. Take one example—this rule requires the designation of a ''privacy official.'' Large health plans dealing with a vast range of information flows may well consider hiring a full time person to oversee compliance with the rule, to assist in planning systems development, and to draft contracts with business partners, among other tasks. A small doctor's office, on the other hand, may instead determine that an existing office manager could oversee the office's privacy policies. There would be no expectation that this small doctor's office hire a full-time privacy official. In each of these examples, the covered entity would be complying with the rule's requirement that a privacy official be designated—but the ways that each complies would reflect the different circumstances of each entity's practice.

It is important for small businesses to understand what their obligations would be and to implement the necessary procedures to comply, with the help of Department's model forms and other resources from professional associations. While most covered

entities would need to be in compliance within two years of the final publication of the rule, small businesses would have an extra year to come into compliance.

Here, we set out the principal (although not exclusive) requirements for small businesses:

1. Notice to Individuals of Information Practices (§ 164.512)

Each covered entity would have to develop a notice of information practices, which, as described above, could be modeled on the form attached to this proposal or on model forms that we expect professional associations to develop. The notice must accurately reflect the entity's practices and include the elements listed in § 164.512.

Covered *health care providers* would have to provide the notice to individuals at first service after the effective date of the rule. Providers are also required to post a current copy of the notice in a clear and prominent location for individuals to see. Covered health *plans* would have to provide the notice to any individual covered by the plan when this rule becomes effective, at enrollment, and after any material change to the notice or at least once every three years.

2. Access of Individuals to Protected Health Information (§ 164.514)

Covered plans and providers would be required to allow individuals to inspect and copy their protected health information. These plans or providers could charge individuals a reasonable cost-based fee for copying.

3. Accounting for Uses and Disclosures (§ 164.515)

Covered plans and providers would have to be able to provide an accounting for uses and disclosures of protected health information for purposes other than treatment, payment, or health care operations. We expect that this burden will be very low for most small businesses, given the nature of most disclosures by such businesses.

4. Amendment and Correction (§ 164.516)

Covered plans and providers would be required to allow individuals to request amendments or corrections to their protected health information.

5. Designated Privacy Official (§ 164.518(a))

Each covered entity would designate a privacy official. As described above, in a small providers office, the office manager may be the official in charge of making sure that the office is implementing its privacy policies and procedures and taking complaints.

6. Training (§ 164.518(b))

All members of covered entities' workforces who have contact with protected health information would be required to have some sort of privacy training about the entity's policies and procedures and to sign a certificate indicating that they had such training. For a small entity, this could simply mean the privacy official briefly discussing how they handle privacy concerns and going over the entity's notice of information practices.

7. Safeguards (§ 164.518(c))

A covered entity would have to establish administrative, technical, and physical safeguards to protect the privacy of protected health information from unauthorized access or use. For a small provider, this may mean having the ability to securely lock up any record that are not being used and ensuring that records are not kept in an area where anyone who is not authorized could view them.

8. Complaints (§ 164.518(d))

Every covered entity would be required to have policies and procedures in place that allow individuals to file complaints about possible privacy violations. For a small entity, this could mean simply that they keep a specific file for complaints.

9. Sanctions (§ 164.518(e))

Covered entities would be required to develop and apply sanctions when a member of a covered entity's work force or business partner fails to comply with the entity's policies and procedures related to this rule. For a small businesses, these could range from requiring a re-training on privacy, to placing a notation of the violation in an employee's record, to dismissal or ending a contract with a business partner.

10. Documentation of Policies and Procedures (§§ 164.520)

Covered entities would be required to document policies and procedures for use and disclosure of protected health information relating to this regulation, including elements listed in § 164.520, and would need to maintain one copy of each version of its notice of information practices, and authorization forms. See § 164.520(f) for a full list of recordkeeping requirements.

11. Minimum Necessary (§ 164.506(b))

When using or disclosing protected health information for treatment, payment, healthcare operations, and other purposes, an entity would be required to disclose only the amount of protected health information necessary to accomplish the intended purpose of the use or disclosure.

12. Business Partners (§ 164.506(e))

For those small businesses that hire ''business partners'' to assist them in carrying out their operations, this rule would require that they take steps, including having certain terms in a contract, to ensure that their business partners are also protecting the privacy of individually identifiable health information. We expect that model contracts will be developed by potential business partners and others that can be used to fulfill the requirements of this section.

13. Special Disclosures That Do Not Require Authorization—Public Health, Research, etc. (§ 164.510)

This proposed rule would also permit disclosure of patients' health information in special cases and under certain conditions. These disclosures would be optional under this proposed rule but may be mandatory under other laws. The primary examples of such permissible disclosures are for: public health purposes, for health oversight purposes, for judicial and administrative proceedings, to coroners and medical examiners, to law enforcement agencies, to next-of-kin, to governmental health data systems, for research purposes, other disclosures required by law, among others. Each of these disclosures and uses would be subject to specific conditions, described in the proposed rule.

14. Verification (§ 164.518(c)(2))

Entities would be required to have reasonable procedures to verify the identity or authority, as applicable, of persons requesting the disclosure of protected health information if the person making the request is not already known to the entity. In most cases, the covered entity could simply ask for a form of identification like a drivers license.

IV. Preliminary Regulatory Impact Analysis

Section 804(2) of title 5, United States Code (as added by section 251 of Public Law 104–121), specifies that a ''major rule'' is any rule that the Office of Management and Budget finds is likely to result in—

- An annual effect on the economy of $100 million or more;
- A major increase in costs or prices for consumers, individual industries,

Federal, State, or local government agencies, or geographic regions; or

- Significant adverse effects in competition, employment, investment productivity, innovation, or on the ability of Unites States based enterprises to compete with foreign-based enterprises in domestic and export markets.

We estimate that the impact of this final rule will be over $1 billion in the first year of implementation. Therefore, this rule is a major rule as defined in Title 5, United States Code, section 804(2).

DHHS has examined the impacts of this proposed rule under Executive Order 12866. Executive Order 12866 directs agencies to assess all costs and benefits of available regulatory alternatives and, when regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects; distributive impacts; and equity). According to Executive Order 12866, a regulatory action is ''significant'' if it meets any one of a number of specified conditions, including having an annual effect on the economy of $100 million or adversely affecting in a material way a sector of the economy, competition, or jobs or if it raises novel legal or policy issues. DHHS finds that this proposed rule is a significant regulatory action as defined by Executive Order 12866. Also in accordance with the provisions of Executive Order 12866, this proposed rule was reviewed by the Office of Management and Budget.

When this proposed rule becomes a final rule, in accordance with the Small Business Regulatory Enforcement and Fairness Act (Pub. L. 104–121), the Administrator of the Office of Information and Regulatory Affairs of the Office of Management and Budget (the Administrator) has determined that this proposed rule would be a major rule for the purpose of congressional review. A major rule for this purpose is defined in 5 U.S.C. 804(2) as one that the Administrator has determined has resulted or is likely to result in an annual effect on the economy of $100 million or more; a major increase in costs or prices for consumers, individual industries, federal State, or local government agencies, or geographic regions; or significant adverse effects on competition, employment, investment, productivity, innovation, or on the ability of U.S.-based enterprises to compete with foreign-based enterprises in domestic or export markets.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) projects a significant increase in the number of medical transactions that will be conducted or transmitted electronically. HIPAA notes the privacy needs that result when individually identifiable health information can be transmitted quickly through electronic information systems. While there is a compelling need to protect the privacy of health information in today's health care system, the expected growth of electronic systems to aide medical diagnostics, claims processing and research makes it even more critical to improve privacy protections.

A fundamental assumption of this regulation is that the greatest benefits of improved privacy protection will be realized in the future as patients gain increasing trust in health care practitioners' ability to maintain the confidentiality of their health information. Furthermore, our analysis rests on the principle that health information privacy is a right, and as such, cannot be valued solely by market costs. Because it is difficult to measure future benefits based on present data, our estimates of the costs and benefits of this regulation are based on the current business environment and do not include projections beyond five years. As a result, we cannot accurately account for all of the regulation's future costs and benefits, but the Department is confident that future benefits will be higher than those stated in this analysis.

In order to achieve a reasonable level of privacy protection, we have three objectives for the proposed rule: (1) To establish baseline standards for health care privacy protection, (2) to establish protection for all health information maintained or transmitted by covered entities, and (3) to protect the privacy of health information that is maintained in electronic form, as well as health information generated by electronic systems.

Establishing minimum standards for health care privacy protection is an attempt to create a baseline level of privacy protection for patients across States. The Health Privacy Project's report, *The State of Health Privacy: An Uneven Terrain*[6] makes it clear that under the current system of state laws, privacy protection is extremely variable. Our statutory authority under HIPAA allows us to preempt state laws when state law provides less stringent privacy protection than the regulation. Only in cases where state law does not protect the patient's health information as stringently as in this proposed rule, or when state law is more restrictive of a patient's right to access their own health care information, will our rule preempt state law. We discuss preemption in greater detail in other parts of the preamble (see the effects of the rule on state laws, section 2 below).

Our second objective is to establish a uniform base of protection for all health information maintained or transmitted by covered entities. As discussed in the preamble, HIPAA restricts the type of entities covered by the proposed rule to three broad categories: health care providers, health care clearinghouses, and health plans. However, there are similar public and private entities that we do not have the authority to regulate under HIPAA. For example, life insurance companies are not covered by this proposed rule but have access to a large amount of protected health information. State government agencies not directly linked to public health functions or health oversight may also have access to protected health information. Examples of this type of agency include the motor vehicle administration, which frequently maintains individual health information, and welfare agencies that routinely hold health information about their clients.

Our third objective is to protect the privacy of health information that is maintained in electronic form, as well as health information generated by electronic systems. Health information is currently stored and transmitted in multiple forms, including in electronic, paper, and oral formats. In order to provide consistent protection to information that has been electronically transmitted or maintained, we propose that this rule cover all personal, protected health information that has ever been maintained or transmitted electronically. This type of information includes output such as computer printouts, X-rays, magnetic tape, and other information that was originally maintained or transmitted electronically. For example, laboratory tests are often computer generated, printed out on paper, and then stored in a patient's record. Because such lab results were originally maintained electronically, the post-electronic (i.e. printed) output of those lab results would also be covered under the proposed rule.

It is important to note that the use of electronic systems to maintain and transmit health information is growing among health care providers, and health plans. Faulkner and Gray report that provider use of electronically processed

[6] Janlori Goldman, Institute for Health Care Research and Policy, Georgetown University: www.healthprivacy.org/resources.

health transactions grew from 47 percent to 62 percent between 1994 and 1998. Payer use of electronic transactions grew 17 percent between 1996 and 1997. Once all of the HIPAA administrative simplification standards are implemented, we expect the number of electronic transactions processed by payers and providers to grow.

The variation in business practice regarding use of paper records versus electronic media for storing and transmitting health information is captured by comparing the percentage of providers that submit paper claims with those that submit electronic claims. Faulkner & Gray's *Health Data Directory* [1] shows that only 40 percent of non-Medicare physician claims and 16 percent of dental claims were submitted electronically in 1998. In contrast, 88 percent of all pharmacy claims were submitted electronically.

We believe that most physicians either have, or will have in the near future, the capacity to submit claims electronically. Faulkner and Gray reported that 81 percent of physicians with Medicare patients submitted their Medicare claims electronically. The difference in the percent of electronic clams submitted to Medicare suggests that the physicians' decisions to submit claims electronically may be heavily influenced by the administrative requirements of the health plan receiving the claim. Since HIPAA requires all health plans to accept electronic transactions and, in order to compete in the technologically driven health care market, more health plans may require electronic claims submissions, physicians will conduct many more electronic transactions in the near future. Therefore, it is extremely important that adequate privacy protections are implemented now.

A. Relationship of This Analysis to Analyses in Other HIPAA Regulations

Historically, Congress has recognized that privacy standards must accompany the electronic data interchange standards and that the increased ease of transmitting and sharing individually identifiable health information must be accompanied by an increase in the privacy and confidentiality. In fact, the majority of the bulk of the first Administrative Simplification section that was debated on the floor of the Senate in 1994 (as part of the Health Security Act) was made up of privacy provisions. Although the requirement for the issuance of concomitant privacy standards remained a part of the bill passed by the House of Representatives, the requirement for privacy standards was removed in conference. This section was moved from the standard-setting authority of Title XI (section 1173 of the Act) and placed in a separate section of HIPAA, section 264. Subsection (b) of section 264 required the Secretary of HHS to develop and submit to the Congress recommendations for:

(1) The rights that an individual who is a subject of individually identifiable health information should have.

(2) The procedures that should be established for the exercise of such rights.

(3) The uses and disclosures of such information that should be authorized or required.

The Secretary's Recommendations were submitted to the Congress on September 11, 1997, and are summarized below. Section 264(c)(1) provides that:

> If legislation governing standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a) of the Social Security Act (as added by section 262) is not enacted by (August 21, 1999), the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than (February 21, 2000). Such regulations shall address at least the subjects described in subsection (b).

As the Congress did not enact legislation governing standards with respect to the privacy of individually identifiable health information prior to August 21, 1999, HHS has now, in accordance with this statutory mandate, developed proposed rules setting forth standards to protect the privacy of such information.

These privacy standards have been, and continue to be, an integral part of the suite of Administrative Simplification standards intended to simplify and improve the efficiency of the administration of our health care system.

The proposed rule should be considered along with all of the administrative simplification standards required by HIPAA. We assessed several strategies for determining the impact of this proposed rule. We considered whether it would be accurate to view the impact as a subset of the overall HIPAA standards or whether this privacy component should be viewed as an addition to the earlier impact analyses related to HIPAA. We decided that while this proposed rule is considered one of the HIPAA standards, any related costs or benefits should be viewed as an addition to earlier analyses. The original HIPAA analyses did not incorporate the expected costs and benefits of privacy regulation because, at the time of the original analyses, we did not know whether Congress would enact legislation or whether privacy would need to be addressed by regulation. Therefore, much of our cost analysis is based on the expected incremental costs above those related to other HIPAA regulations.

B. Summary of Costs and Benefits.

The Department has estimated the costs and benefits of the proposed rule based on several caveats. In general, it is difficult to estimate the costs and benefits of improved privacy protection. The ability to measure costs of the proposed regulation is limited because there is very little data currently available on the cost of privacy protection. The Department has not been able to estimate costs for a number of requirements of the proposed regulation that we know will impose some cost to covered entities. For those elements for which there are estimated costs, data and information limitations limit the precision of the Department's estimates; for those reasons we have provided an overall range of costs in addition to point estimates, and welcome further information from the public as part of the comment process. Furthermore, the number of new privacy requirements that the regulation will introduce to the health care industry exacerbates difficulties estimating the benefits of privacy. Benefits are difficult to measure because we conceive of privacy primarily as a right and secondarily as a commodity. As discussed below, the significant benefits of the proposed regulation to individuals and society can be demonstrated by illustrating the serious privacy concerns raised by mental health, substance abuse, cancer screening, and HIV/AIDS patients and the benefits that may be derived from greater privacy.

The estimated cost of compliance with the proposed rule would be at least $3.8 billion over five years. The cost includes estimates for the majority of the requirements of the proposed regulation, but not all. These estimates include costs to federal, State, and local governments. Federal, and State and local costs are therefore a subset of total costs. Based on a plausible range of costs for the key components of the analysis, the cost of the regulation would likely be in the range $1.8 to $6.3 billion over five years (not including those elements of the regulation for

[1] Health Data Directory, Faulkner & Gray; 1999 Edition, pp 22–23.

which we could not make any cost estimates).

The compliance costs are in addition to Administrative Simplification estimates. The cost of complying with the privacy regulation represents about 0.09 percent of projected national health expenditures during the first year following the regulation's enactment. The five-year cost of the proposed regulation also represents 1.0 percent of the increase in health care costs that will occur during the same five-year period.[8]

The largest cost item is the amending and correcting of records, which would represent over one-half of total costs. Provider and plan notices, which we estimate would cost $439 million, is the second largest cost, and inspection and copying of records is estimated to be $405 million. The one-time costs for providers to develop policies and procedures represent somewhat less than 10 percent of the total cost, or $333 million. Plans would bear a substantially smaller cost—approximately $62 million. Other systems changes would cost about $90 million over the period. The cost of administering written authorizations would total approximately $271 million over five years.

The cost estimates include private- and public-sector costs. Many of the public-sector cost elements will be the same as those in the private market. However, privacy notices are likely to represent a smaller fraction of total public-sector costs, while systems compliance costs in the public sector may be higher than in the private sector due to oversight and administrative requirements.

The costs presented in this document are the Department's best estimates of the cost of implementing the proposed regulation based on available information and data. Because of inadequate data, we have not made cost estimates for the following components of the regulation: The principle of minimum necessary disclosure; the requirement that entities monitor business partners with whom they share PHI; creation of de-identified information; internal complaint processes; sanctions; compliance and enforcement; the designation of a privacy official and creation of a privacy board; and additional requirements on research/optional disclosures that will be imposed by the regulation. The cost of these provisions may be significant in some cases, but it would be inaccurate to project costs for these requirements given the fact that several of these concepts are new to the industry, and there is little direct evidence on costs. We solicit comment regarding costs of the regulation that we have not quantified.

The privacy protections established by this regulation will provide major social benefits. Establishing privacy protection as a fundamental right is an important goal and will have significant, non-quantifiable social benefits. A well-designed privacy standard can be expected to build confidence among the public about the confidentiality of their health information. Increased confidence in the privacy of an individual's health information can be expected to increase the likelihood that many people will seek treatment for particular classes of disease, particularly mental health conditions, sexually transmitted diseases such as HIV/AIDS, and earlier screening for certain cancers. The increased utilization of medical services that would result from increased confidence in privacy would lead to improved health for the individuals involved, reduced costs to society associated with delayed treatments, and improved public health attributable to reduced transmission of communicable diseases.

TABLE 1.—THE COST OF COMPLYING WITH THE PROPOSED PRIVACY REGULATION

[In dollars]

Provision	Initial or first year cost (2000)	Annual cost after the first year	Five year (2000–2004) cost
Development of Policies and Procedures—Providers (totaling 871,294)	$333,000,000	.....	$333,000,000
Development of Policies and Procedures—Plans (totaling 18,225)	62,000,000	.....	62,000,000
System Changes—All Entities	90,000,000	.....	90,000,000
Notice Development Cost—All Entities	20,000,000	.....	30,000,000
Notice Issuance—Providers	59,730,000	37,152,000	208,340,000
Notice Issuance—Plans	46,200,000	46,200,000	231,000,000
Inspection/Copying	81,000,000	81,000,000	405,000,000
Amendment/Correction	407,000,000	407,000,000	2,035,000,000
Written Authorization	54,300,000	54,300,000	271,500,000
Paperwork/Training	22,000,000	22,000,000	110,000,000
Other Costs*	**N/E	N/E	N/E
Total	$1,165,230,000	$647,652,000	$3,775,840,000

*Other Costs include: minimum necessary disclosure; monitoring business partners with whom entities share PHI; creation of de-identified information; internal complaint processes; sanctions; compliance and enforcement; the designation of a privacy official and creation of a privacy board; additional requirements on research/optional disclosures that will be imposed by the regulation.

**N/E = ''Not estimated''.

We promote the view that privacy protection is an important personal right, and suggest that the greatest of the benefits of the proposed regulation are impossible to estimate based on the market value of health information alone. However, it is possible to evaluate some of the benefits that may accrue to individuals as a result of proposed regulation, and these benefits, alone, demonstrate that the regulation is warranted.

These benefits are considered both qualitatively and quantitatively. As a framework for the discussion, the cost of the provisions in the regulation that have been quantified is $0.46 per health care encounter. Although the value of privacy cannot be fully calculated, it is worth noting that if individuals would be willing to pay more than $0.46 per health care encounter to improve health information privacy, the benefits of the

[8] Health Care Finance Administration, Office of the Actuary, 1997.

proposed regulation would outweigh the cost.

Several qualitative examples illustrate the benefits of the proposed regulation. In one case, medical privacy concerns may prevent patients from obtaining early testing and screening for certain types of cancer. Of types of cancer for which screening is available, survival rates might increase to 95 percent diagnosed in the early stages [9]. For HIV/AIDS patients, new treatments for patients who are diagnosed with HIV in the early stages may save $23,700 per quality-adjusted year of life saved [10]. Later in this document, the potential to reduce illness and disability associated with sexually transmitted diseases is discussed.

We recognize that many of the costs and benefits of health information privacy are difficult to quantify, but we believe that our estimates represent a reasonable range of the economic costs and benefits associated with the regulation.

C. Need for the Proposed Action.

Privacy is a fundamental right. As such, it has to be viewed differently than any ordinary economic good. Although the costs and benefits of a regulation need to be considered as a means of identifying and weighing options, it is important not to lose sight of the inherent meaning of privacy: it speaks to our individual and collective freedom.

A right to privacy in personal information has historically found expression in American law. All fifty states today recognize in tort law a common law or statutory right to privacy. Many states specifically provide a remedy for public revelation of private facts. Some states, such as California and Tennessee, have a right to privacy as a matter of state constitutional law. The multiple historical sources for legal rights to privacy are traced in many places, including Chapter 13 of Alan Westin's Privacy and Freedom and in Ellen Alderman & Caroline Kennedy, The Right to Privacy (1995).

To take but one example, the Fourth Amendment to the United States Constitution guarantees that ''the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated.'' By referring to the need for security of ''persons'' as well as ''papers and effects'' the Fourth Amendment suggests enduring values in American law that relate to privacy. The need for security of ''persons'' is consistent with getting patient consent before performing invasive medical procedures. The need for security in ''papers and effects'' underscores the importance of protecting information about the person, contained in sources such as personal diaries, medical records, or elsewhere. As is generally true for the right of privacy in information, the right is not absolute. The test instead is what constitutes an ''unreasonable'' search of the papers and effects.

The United States Supreme Court has specifically upheld the constitutional protection of personal health information. In *Whalen* v. *Roe,* 429 U.S. 589 (1977), the Court analyzed a New York statute that created a database of persons who obtained drugs for which there was both a lawful and unlawful market. The Court, in upholding the statute, recognized at least two different kinds of interests within the constitutionally protected ''zone of privacy.'' ''One is the individual interest in avoiding disclosure of personal matters,'' such as this proposed regulation principally addresses. This interest in avoiding disclosure, discussed in *Whalen* in the context of medical information, was found to be distinct from a different line of cases concerning ''the interest in independence in making certain kinds of important decisions.'' In the recent case of *Jaffee* v. *Redmond,* 116 S.Ct. 1923 (1996), the Supreme Court held that statements made to a therapist during a counseling session were protected against civil discovery under the Federal Rules of Evidence. The Court noted that all fifty states have adopted some form of the psychotherapist-patient privilege. In upholding the federal privilege, the Supreme Court stated that it ''serves the public interest by facilitating the appropriate treatment for individuals suffering the effects of a mental or emotional problem. The mental health of our citizenry, no less than its physical health, is a public good of transcendent importance.''

Many writers have urged a philosophical or common-sense right to privacy in one's personal information. Examples include Alan Westin, Privacy and Freedom (1967) and Janna Malamud Smith, Private Matters: In Defense of the Personal Life (1997). These writings emphasize the link between privacy and freedom and privacy and the ''personal life,'' or the ability to develop one's own personality and self-expression. Smith, for instance, states:

> The bottom line is clear. If we continually, gratuitously, reveal other people's privacies, we harm them and ourselves, we undermine the richness of the personal life, and we fuel a social atmosphere of mutual exploitation. Let me put it another way: Little in life is as precious as the freedom to say and do things with people you love that you would not say or do if someone else were present. And few experiences are as fundamental to liberty and autonomy as maintaining control over when, how, to whom, and where you disclose personal material. Id. at 240–241.

Individuals' right to privacy in information about themselves is not absolute. It does not, for instance, prevent reporting of public health information on communicable diseases or stop law enforcement from getting information when due process has been observed. But many people believe that individuals should have some right to control personal and sensitive information about themselves.

Among different sorts of personal information, health information is among the most sensitive. Many people believe that details about their physical self should not generally be put on display for neighbors, employers, and government officials to see. Informed consent laws place limits on the ability of other persons to intrude physically on a person's body. Similar concerns apply to intrusions on information about the person. Moving beyond these facts of physical treatment, there is likely a greater intrusion when the medical records reveal details about a person's mental state, such as during treatment for mental health. If, in Justice Brandeis' words, the ''right to be let alone'' means anything, then it likely applies to having outsiders have access to one's intimate thoughts, words, and emotions.

In addition to these arguments based on the right to privacy in personal information, market failures will arise to the extent that privacy is less well protected than the parties would have agreed to, if they were fully informed and had the ability to monitor and enforce contracts. The chief market failures with respect to privacy concern information, negotiating, and enforcement costs. The information costs arise because of the information asymmetry between the company and the patient—the company typically knows far more than the patient about how the information will be used by that company. A health care provider or plan, for instance, knows many details about how protected health information will be generated, combined with other databases, or sold to third parties.

---

[9] American Cancer Society. http://www.cancer.org/statistics/97cff/97facts.html

[10] John Hornberger et al, ''Early treatment with highly active anti-retroviral therapy (HAART) is cost-effective compared to delayed treatment,'' 12th World AIDS conference, 1998.

Patients face at least two layers of cost in learning about how their information is used. First, as with many aspects of health care, patients face the challenge of trying to understand technical medical terminology and practices. It will often be difficult for a patient to understand the medical records and the implications of transferring various parts of such records to a third party. Second, especially in the absence of consistent national rules, patients may face significant costs in trying to learn and understand the nature of a company's privacy policies.

The costs of learning about companies' policies are magnified by the difficulty patients face in detecting whether companies in fact are complying with those policies. Patients might try to adopt strategies for monitoring whether companies have complied with their announced policies. For instance, if a person received health care from several providers that promised not to sell her name to third parties, she could report a different middle initial to each provider. She could then identify the provider that broke the agreement by noticing the middle initials that later appeared on an unsolicited marketing letter. These sorts of strategies, however, are both costly (in time and effort) and likely to be ineffective. A company using the patient's name, for instance, could cross-check her address with her real name, and thereby insert the correct middle initial. In addition, modern health care often requires protected health information to flow legitimately among multiple entities for purposes of treatment, payment, health care operations, and other necessary uses. Even if the patient could identify the provider whose data ultimately leaked, the patient could not easily tell which of those multiple entities had impermissibly transferred her information.

The cost and ineffectiveness of monitoring logically leads to less than optimal protection of health information. Consider the incentives facing a company that acquires protected health information. That company gains the full benefit of using the information, including in its own marketing efforts or in the fee it can receive when it sells the information to third parties. The company, however, does not suffer the full losses from disclosure of protected health information. Because of imperfect monitoring, customers often will not learn of, and thus not be able to enforce against, that unauthorized use. They will not be able to discipline the company efficiently in the marketplace for its less-than-optimal privacy practices. Because the company internalizes the gains from using the information, but does not bear a significant share of the cost to patients (in terms of lost privacy), it will have a systematic incentive to over-use protected health information. In market failure terms, companies will have an incentive to use protected health information where the patient would not have freely agreed to such use.

These difficulties in contract enforcement are made worse by the third-party nature of many health insurance and payment systems. Even where individuals would wish to bargain for privacy, they may lack the legal standing to do so. For instance, employers often negotiate the terms of health plans with insurers. The employee may have no voice in the privacy or other terms of the plan, facing a take-it-or-leave-it choice of whether to be covered by insurance. The incentive of employers may be contrary to the wishes of employees—employers may in some cases inappropriately insist on having access to sensitive medical information in order to monitor employees' behavior and health status. In light of these complexities, there are likely significant market failures in the bargaining on privacy protection. Many privacy-protective agreements that patients would wish to make, absent barriers to bargaining, will not be reached. The economic, legal and philosophical arguments become more compelling as the medical system shifts from predominantly paper to predominantly electronic records. From an economic perspective, market failures will arise to the extent that privacy is less well protected than the parties would have agreed to, if they were fully informed and had some equality of bargaining power. The chief market failures with respect to privacy concern information and bargaining costs. The information costs arise because of the information asymmetry between the company and the patient—the company typically knows far more than the patient about how the information will be used by that company. A health care provider or plan, for instance, knows many details about how protected health information will be generated, combined with other databases, or sold to third parties.

Rapid changes in information technology mean that the size of the market failures will likely increase greatly in the markets for personal health information. Improvements in computers and networking mean that the costs of gathering, analyzing, and disseminating electronic data are plunging. Market forces are leading many medical providers and plans to shift from paper to electronic records, due both to lower cost and the increased functionality provided by having information in electronic form. These market changes will be accelerated by the administrative simplification implemented by the other regulations promulgated under HIPAA. A chief goal of administrative simplification, in fact, is to create a more efficient flow of medical information where appropriate. This proposed privacy regulation is an integral part of the overall effort of administrative simplification; it creates a framework for more efficient flows for certain purposes, including treatment and payment, while restricting flows in other circumstances except where appropriate institutional safeguards exist.

If the medical system shifts to predominantly electronic records in the near future, without use of accompanying privacy rules, then one can imagine a near future where clerical and medical workers all over the country may be able to pull up protected health information about individuals—without meaningful patient consent and without effective institutional controls against further dissemination. In terms of the market failure, it will become more difficult for patients to know how their health provider or plan is using their personal health information. It will become more difficult to monitor the subsequent flows of protected health information, as the number of electronic flows and possible points of leakage both increase. Similarly, the costs and difficulties of bargaining to get the patients' desired level of use will likely rise due the greater number and types of entities that receive protected health information.

As the benefits section, below, discusses in more detail, the protection of privacy and correcting the market failure have practical implications. Where patients are concerned about lack of privacy protections, they might fail to get medical treatment that they would otherwise seek. This failure to get treatment may be especially likely for certain conditions, including mental health, substance abuse, and conditions such as HIV. Similarly, patients who are concerned about lack of privacy protections may report inaccurately to their providers when they do seek treatment. For instance, they might decide not to mention that they are taking prescription drugs that indicate that they have an embarrassing condition. These inaccurate reports may lead to mis-diagnosis and less-than-optimal treatment, including

inappropriate additional medications. In short, the lack of privacy safeguards can lead to efficiency losses in the form of foregone or inappropriate treatment.

The shift from paper to electronic records, with the accompanying greater flows of sensitive health information, also strengthens the arguments for giving legal protection to the right to privacy in protected health information. In an earlier period where it was far more expensive to access and use medical records, the risk of harm to individuals was relatively low. In the potential near future, where technology makes it almost free to send lifetime medical records over the Internet, the risks may grow rapidly. It may become cost-effective, for instance, for companies to offer services that allow purchasers to obtain details of a person's physical and mental treatments. In addition to legitimate possible uses for such services, malicious or inquisitive persons may download medical records for purposes ranging from identity theft to embarrassment to prurient interest in the life of a celebrity or neighbor. Of additional concern, such services might extend to providing detailed genetic information about individuals, without their consent. Many persons likely believe that they have a right to live in society without having these details of their lives laid open to unknown and possibly hostile eyes. These technological changes, in short, may provide a reason for institutionalizing privacy protections in situations where the risk of harm did not previously justify writing such protections into law.

States have, to varying degrees, attempted to enhance confidentiality and correct the market problems by establishing laws governing at least some aspects of medical record privacy. This approach, though a step in the right direction, is inadequate. The states themselves have a patch quilt of laws that fail to provide a consistent or comprehensive policy, and there is considerable variation among the states in the scope of the protections provided. Moreover, health data is becoming increasingly ''national''; as more information becomes available in electronic form, it can have value far beyond the immediate community where the patient resides. Neither private action nor state laws provide a sufficiently rigorous legal structure to correct the market failure now or in the future. Hence, a national policy with consistent rules is a vital step toward correcting the market failure that exists.

In summarizing the need for the proposed regulation, the discussion here has emphasized how the proposed regulation would address violations of a right to privacy in the information about oneself, market failures, and the need for a national policy. These arguments become considerably stronger with the shift from predominantly paper to predominantly electronic records. Other arguments could supplement these justifications. As discussed in the benefits section below, the proposed privacy protections may prevent or reduce the risk of unfair treatment or discrimination against vulnerable categories of persons, such as those who are HIV positive, and thereby, foster better health. The proposed regulation may also help educate providers, plans, and the general public about how protected health information is used. This education, in turn, may lead to better information practices in the future.

Clearly, the growing problem of protecting privacy is widely understood and a major public concern. Over 80 percent of persons surveyed in 1999 agreed with the statement that they had ''lost all control over their personal information.'' A Wall Street Journal/NBC poll on September 16, 1999 asked Americans what concerned them most in the coming century. ''Loss of personal privacy'' topped the list, as the first or second concern of 29 percent of respondents. Other issues such as terrorism, world war, and global warming had scores of 23 percent or less. The regulation is a major step toward addressing this public concern.

D. Baseline Privacy Protections

Determining the impact of the rule on covered entities requires us to establish a baseline for current privacy policies. We must first determine current practices and requirements related to protected information—specifically, practices related to disclosure and use, notification of individuals of information practices, inspection and copying, amendment and correction, administrative policies, procedures, and related documentation.

Privacy practices are most often shaped by professional organizations that publish ethical codes of conduct and by State law. On occasion, State laws defer to professional conduct codes. At present, where neither professional organizations nor States have developed guidelines for privacy practices, an entity may implement privacy practices independently.

Professional codes of conduct or ethical behavior generally can be found as opinions and guidelines developed by organizations such as the American Medical Association, the American Hospital Association, and the American Dental Association. These are generally issued though an organization's governing body. The codes do not have the force of law, but providers often recognize them as binding rules.

State laws are another important means of protecting health information. While professional codes of conduct usually only have slight variations, State laws vary dramatically. Some States defer to the professional codes of conduct, others provide general guidelines for privacy protection, and others provide detailed requirements relating to the protection of information relating to specific diseases or to entire classes of information. In cases where neither State law nor professional ethical standards exist, the only privacy protection individuals have is limited to the policies and standards that the health care entity adopts.

Before we can attempt to determine the impact of the proposed rule on covered entities, we must make an effort to establish the present level of privacy protection. Current privacy protection practices are determined by the standards and practices that the professional associations have adopted for their members and by State laws.

1. Professional Codes of Conduct and the Protection of Health Information

We examined statements issued by five major professional groups, one national electronic network association and a leading managed care association. There are a number of common themes that all the organizations appear to subscribe to:

- The need to maintain and protect an individual's health information;
- Development of policies to ensure the confidentiality of protected health information;
- Only the minimum necessary information should be released to accomplish the purpose for which the information is sought.

Beyond these principles, the major associations differ with respect to the methods used to protect health information. One critical area of difference is the extent to which professional organizations should release protected health information. A major mental health association advocates the release of identifiable patient information ''* * * only when de-identified data are inadequate for the purpose at hand.'' A major association of physicians counsels members who use electronically maintained and transmitted data to require that they and their patients know in advance who has access to protected patient data, and the purposes for which the data will be

used. In another document, the association advises physicians not to ''sell'' patient information to data collection companies without fully informing their patients of this practice and receiving authorization in advance to release of the information.

Only two of the five professional groups state that patients have the right to review their medical records. One group declares this as a fundamental patient right, while the second association qualifies their position by stating that the physician has the final word on a patient's access to their health information. This association also recommends that its members respond to requests for access to patient information within 10 days, and recommends that entities allow for an appeal process when patients are denied access. The association further recommends that when a patient contests the accuracy of the information in their record and the entity refuses to accept the patient's change, the patient's statement should be included as a permanent part of the patient's record.

In addition, three of the five professional groups endorse the maintenance of audit trails that can track the history of disclosures of protected health information.

The one set of standards that we reviewed from a health network association advocated the protection of private health information from disclosure without patient authorization and emphasized that encrypting information should be a principal means of protecting patient information. The statements of a leading managed care association, while endorsing the general principles of privacy protection, were vague on the release of information for purposes other than treatment. They suggest allowing the use of protected health information without the patient's authorization for what they term ''health promotion.'' It is possible that the use of protected health information for ''health promotion'' may be construed under the proposed rule as part of marketing activities.

Based on the review of the leading association standards, we believe that the proposed rule embodies all the major principles expressed in the standards. However, there are some major areas of difference between the proposed rule and the professional standards reviewed. These include the subject individual's right of access to health information in the covered entity's possession, relationships between contractors and covered entities, and the requirement that covered entities make their privacy policies and practices available to patients through a notice and the ability to respond to questions related to the notice. Because the proposed regulation would require that (with a few exceptions) patients have access to their health information that a covered entity possesses, large numbers of providers may have to modify their current practices in order to allow patient access, and to establish a review process if they deny a patient access. Also, none of the privacy protection standards reviewed require that providers or plans prepare a formal statement of privacy practices for patients (although the major physician association urges members to inform patients about who would have access to their protected health information and how their health information would be used). Only one HMO association explicitly made reference to information released for legitimate research purposes, and none of the other statements we reviewed discuss release of information for research purposes. The proposed rule allows for the release of protected health information for research purposes without an individual's authorization, but only for research that is supervised by an institutional research board or an equivalent privacy board. This research requirement may cause some groups to revise their disclosure authorization standards.

2. State Laws

The second body of privacy protections is found in a myriad of State laws and requirements. To determine whether or not the proposed rule would preempt a State law, we first identified the relevant laws, and second, determined whether state or federal law provides individuals with greater privacy protection.

Identifying the relevant state statutes: Health privacy statutes can be found in laws applicable to many issues including insurance, worker's compensation, public health, birth and death records, adoptions, education, and welfare. For example, Florida has over 60 laws that apply to protected health information. According to the Georgetown Privacy Project [11], Florida is not unique. Every State has laws and regulations covering some aspect of medical information privacy. In many cases, State laws were enacted to address a specific situation, such as the reporting of HIV/AIDS, or medical conditions that would impair a person's ability to drive a car. Identifying every State statute, regulation, and court case that interprets statutes and regulations dealing with patient medical privacy rights is an important task but cannot be completed in this discussion. For the purpose of this analysis, we simply acknowledge the complexity of State requirements surrounding privacy issues.

Lastly, we recognize that the private sector will need to complete a State-by-State analysis to comply with the notice and administrative procedures portion of this proposed rule. This comparison should be completed in the context of individual markets; therefore it is more efficient for professional associations or individual businesses to complete this task.

Recognizing limits of our ability to effectively summarize State privacy laws and our difficulty in determining preemption at the outset, we discuss conclusions generated by the Georgetown University Privacy Project in Janlori Goldman's report, *The State of Health Privacy: An Uneven Terrain*. We consider Georgetown's report the best and most comprehensive examination of State privacy laws currently published. The report, which was completed in July 1999, is based on a 50-state survey. However, the author is quick to point out that this study is not exhaustive.

The following analysis of State privacy statutes and our attempt to compare State laws to the proposed rule is limited as a result of the large amount of State-specific data available. To facilitate discussion, we have organized the analysis into two sections: access to medical information and disclosure of medical information. Our analysis is intended to suggest areas where the proposed rule appears to preempt various State laws; it is not designed to be a definitive or wholly comprehensive State-by-State comparison.

Access to Subject's Information: In general, State statutes provide individuals with access to their own medical records. However, only a few States allow individuals access to virtually all entities that hold health information. In 33 States, individuals may access their hospital and health facility records. Only 13 States guarantee individuals access to their HMO records, and 16 States provide individuals access to their medical information when it is held by insurers. Seven states have no statutory right of patient access; three States and the District of Columbia have laws that only assure individuals' right to access their mental health records. Only one State permits individuals access to records held by providers, but it excludes pharmacists from the definition of provider. Thirteen States grant individuals statutory right of access to pharmacy records.

[11] *Ibid*, Goldman, p. 6.

The amount that entities are allowed to charge for copying of individuals' records varies widely from State to State. A study conducted by the American Health Information Management Association [12] found considerable variation in the amounts, structure, and combination of fees for search and retrieval, and the copying of the record.

In 35 States, there are laws or regulations that set a basis for charging individuals inspecting and copying fees. Charges vary not only by State, but also by whether the request is related to a worker's compensation case or a patient-initiated request. Charges also vary according to the setting. For example, States differentiate most often between clinics and hospitals. Also, charges vary by the number of pages and whether the request is for X-rays or for standard medical information.

Of the 35 States with laws regulating inspection and copying charges, seven States either do not allow charges for retrieval of records or require that the entity provide the first copy free of charge. Some States may prohibit hospitals from charging patients a retrieval and copying fee, but allow clinics to do so. It is noteworthy that some States that do not permit charges for retrieval sometimes allow entities to charge per-page rates ranging between $0.50 and $0.75. In States that do allow a retrieval charge, the per-page charge is usually $0.25. Eleven states specify only that the record holder may charge ''reasonable/actual costs.''

Of the States that allow entities to charge for record retrieval and copying, charges range from a flat amount of $1.00 to $20.00. Other States allow entities to charge varying rates depending on the amount of material copied. For example, an entity may charge $5.00 for the first five pages and then a fixed amount per page. In those cases, it appears that retrieval and copying costs were actually combined. The remaining States have a variety of cost structures: One State allows $0.25 per page plus postage plus a $15.00 retrieval charge. Another State allows a $1.00 charge per page for the first 25 pages and $0.25 for each page above 25 pages plus a $1.00 annual retrieval charge. A third state allows a $1.00 per page charge for the first 100 pages and $0.25 for each page thereafter.

According to the report by the Georgetown Privacy Project, among States that do grant access to patient records, the most common basis for denying individuals access is concern for the life and safety of the individual or others. This proposed rule considers the question of whether to deny patient access on the basis of concern for the individual's life or safety, concluding that the benefits of patient access most often outweigh harm to the individual. This issue, which is discussed in greater detail in other sections, has been resolved in favor of promoting patient access.

The amount of time an entity is given to supply the individual with his or her record varies widely. Many States allow individuals to amend or correct inaccurate health information, especially information held by insurers. However, few States provide the right to insert a statement in the record challenging the covered entity's information when the individual and entity disagree.[13]

Disclosure of Health Information: State laws vary widely with respect to disclosure of identifiable health information. Generally, States have applied restrictions on the disclosure of health information either to specific entities or to specific health conditions. Just two states place broad limits on disclosure of protected health information without regard for policies and procedures developed by covered entities. Most States require patient authorization before an entity may disclose health information, but as the Georgetown report points out, ''In effect, the authorization may function more as a waiver of consent—the patient may not have an opportunity to object to any disclosures.'' [14]

It is also important to point out that none of the States appear to offer individuals the right to restrict disclosure of their protected health information for treatment. Thus, the provision of the proposed rule that allows patients to restrict disclosure of the their protected information is not currently included in any State law. Because the ability to restrict disclosure currently is not a standard practice, the proposed rule would require entities to add these capabilities to their information systems.

State statutes often have exceptions to requiring authorization before disclosure. The most common exceptions are for purposes of treatment, payment, or auditing and quality assurance functions—which are similar to the definition we have established for health care operations, are therefore not subject to prior authorization requirements under the proposed rule. Restrictions on re-disclosure of protected health information also vary widely from State to State. Some States restrict the re-disclosure of health information, and others do not. The Georgetown report cites State laws that require providers to adhere to professional codes of conduct and ethics with respect to disclosure and re-disclosure of protected health information. What is not clear is the degree to which individual information is improperly released or used in the absence of specific legal sanctions.

Most States have adopted specific measures to provide additional protections with regard to certain conditions or illnesses that have clear social or economic consequences. Although the Georgetown study does not indicate the number of States that have adopted disease-specific measures to protect information related to sensitive conditions and illnesses, the analysis seems to suggest that nearly all States have adopted some form of additional protection. The conditions and illnesses most commonly afforded added privacy protection are:

- Substance abuse;
- Information derived from genetic testing;
- Communicable and sexually-transmitted diseases;
- Mental health; and
- Abuse, neglect, domestic violence, and sexual assault.

We have included a specific discussion of disclosures for research purposes because if an entity decides to disclose information for research purposes, it will incur costs that otherwise would be associated with other disclosures under this rule. Some States place restrictions on releasing condition-specific health information for research purposes, while others allow release of information for research without the patient's authorization. States frequently require that researchers studying genetic diseases, HIV/AIDS, and other sexually transmitted diseases have different authorization and privacy controls than those used for other types of research. Some States require approval from an IRB or agreements that the data will be destroyed or identifiers removed at the earliest possible time. Another approach has been for States to require researchers to obtain sensitive, identifiable information from a State public health department. One State does not allow automatic release of protected health information for research purposes without notifying the subjects that their health information may be used in research and allowing

[12] ''Practice Briefs,'' Journal of AHIMA; Harry Rhodes, Joan C. Larson, Association of Health Information Outsourcing Service; January 1999.

[13] Ibid, Goldman, p.20.

[14] Ibid, Goldman, p. 21.

them opportunity to object to the use of their information.[15]

Comparing State statutes to the proposed rule: A comparison of State privacy laws with the proposed rule highlights several of the proposed rule's key implications:

- No State law requires covered entities to make their privacy and access policies available to patients. Thus, all covered entities that have direct contact with patients will be required to prepare a statement of their privacy protection and access policies. This necessarily assumes that entities have to develop procedures if they do not already have them in place.
- The proposed rule will affect more entities than are affected under many State laws. In the application of the proposed rule to providers, plans, and clearinghouses, the proposed rule will reach nearly all entities involved in delivering and paying for health care. Yet because HIPAA applies only to information that has been stored and transmitted electronically, the extent to which the proposed rule will reach information held by covered entities is unclear.
- State laws have not addressed the form in which health information is stored. We do not know whether covered entities will choose to treat information that never has been maintained or transmitted electronically in the same way that they treat post-electronic information. We also do not know what portion of information held in non-electronic formats has ever been electronically maintained or transmitted. Nevertheless, the proposed rule would establish a more level floor from which States could expand the privacy protections to include both electronic information and non-electronic information.
- Among the three categories of covered entities, it appears that plans will be the most significantly affected by the access provisions of the proposed rule. Based on the Health Insurance Association of America (HIAA) data,[16] there are approximately 94.7 million non-elderly persons who purchase health insurance in the 35 States that do not provide patients a legal right to inspect and copy their records. We do not have information on how many of those people are in plans that grant patients inspection and copying rights although State law does not require them to do so. We discuss these points more fully in the cost analysis section.
- Although the proposed rule would establish a uniform disclosure and re-disclosure requirement for all covered entities, the groups most likely to be affected are health insurers, benefits management administrators, and managed care organizations. These groups have the greatest ability and economic incentives to use protected health information for marketing services to both patients and physicians without individual authorization. Under the proposed rule, covered entities would have to obtain the individual's authorization before they could use or disclose their information for purposes other than treatment, payment, and health care operations—except in the situations explicitly defined as allowable disclosures without authorization.
- While our proposed rule appears to encompass many of the requirements found in current State laws, it also is clear that within State laws, there are many provisions that cover specific cases and health conditions. Certainly, in States that have no research disclosure requirements, the proposed rule will establish a baseline standard. But in States that do place conditions on the disclosure of protected health information, the proposed rule may place additional requirements on covered entities.
- State privacy laws do not always apply to entities covered by the proposed rule. For example, State laws may provide strong privacy protection for hospitals and doctors but not for dentists or HMOs. State laws protecting particular types of genetic testing or conditions may be similarly problematic because they protect some types of sensitive information and not others. In some instances, a patient's right to inspect his or her medical record may be covered under State laws and regulations when a physician has the medical information, but not under State requirements when the information being sought is held by a plan. Thus, the proposed rule would extend privacy requirements already applicable to some entities within a State to other entities that currently are not subject to State privacy requirements.

3. Federal Laws

The Privacy Act of 1974. Federal agencies will be required to comply with both the Privacy Act of 1974 (5 U.S.C. 552a) and the HIPAA regulation. The Privacy Act provides Federal agencies with a framework and scheme for protecting privacy, and the HIPAA regulation will not alter that scheme. Basic organizational and management features, such as the provision of safeguards to protect the privacy of health information and training for employees—which are required by this proposed rule—already are required by the Privacy Act.

The proposed rule has been designed so that individuals will not have fewer rights than they have now under the Privacy Act. It may require that agencies obtain individual authorization for some disclosures that they now make without authorization under routine uses.

Private-sector organizations with contracts to conduct personal data handling activities for the Federal government are subject to the Privacy Act by virtue of performing a function on behalf of a Federal agency. They too will be required to comply with both rules in the same manner as Federal agencies.

Substance Abuse Confidentiality Statute. Organizations that operate specialized substance abuse treatment facilities and that either receive Federal assistance or are regulated by a Federal agency are subject to confidentiality rules established by section 543 of the Public Health Service Act (42 U.S.C. 290dd–2) and implementing regulations at 42 CFR part 2.

These organizations will be subject both to that statute and to the HIPAA regulation. The proposed rule should have little practical effect on the disclosure policies of these organizations, because the patient confidentiality statute governing information about substance abuse is generally more restrictive than this proposed rule. These organizations will continue to be subject to current restrictions on their disclosures. The substance abuse confidentiality statute does not address patient access to records; the proposed privacy rule makes clear that patient access is allowed.

Federal agencies are subject to these requirements, and currently they administer their records under both these requirements and the Privacy Act. The Department of Veterans Affairs is subject to its own substance abuse confidentiality statute, which is identical in substance to the one of more general applicability. It also covers information about HIV infection and sickle cell anemia (38 U.S.C. 7332).

Rules Regarding Protection of Human Subjects. Health care delivered by covered entities conducting clinical trials typically are subject to both the

[15] ''Medical records and privacy: empirical effects of legislation; A memorial to Alice Hersh'; McCarthy, Douglas B; Shatin, Deborah; *et al. Health Service Research:* April 1, 1999; No. 1, Vol. 34; p. 417. The article details the effects of the Minnesota law conditioning disclosure of protected health information on patient authorization.

[16] *Source Book of Health Insurance Data: 1997–1998*, Health Insurance Association of America, 1998. p. 33.

proposed rule and to Federal regulations for protection of human re search subjects (The Federal Policy for the Protection of Human Subjects, codified for the Department of Health and Human Services in Title 45 CFR part 46, and/or the Food and Drug Administration's human subject regulations for research in support of medical product applications to the Food and Drug Administration, or regulated by that agency, at 21 CFR parts 50 and 56).

Current human subjects rules impose no substantive restrictions on disclosure of patient information. Institutional review boards must consider the adequacy of confiden tiality protections for subjects, and researchers must tell subjects to what extent their con fidentiality will be protected. There should be no conflict between these requirements and the proposed rules. The proposed HIPAA regulation will expand on the current human subjects requirements by requiring a more detailed description of intended use of patient information. The proposed HIPAA rule also requires additional criteria for waiver of patient authorization.

Medicaid. States may use information they obtain in the process of administering Medicaid only for the purposes of administering the program, pursuant to a State plan condition in section 1902(a)(7) of the Social Security Act, 42 U.S.C. 1396a(a)(7). The proposed HIPAA rule applies to State Medicaid programs, which under the rule are considered health plans. There will be no conflict in the substantive requirements of current rules and this proposed rule. Medicaid rules regarding disclosure of patient information are stricter than provisions of the proposed rule; therefore, Medicaid agencies simply will continue to follow the Medicaid rules.

ERISA. ERISA (29 U.S.C. 1002) was enacted in 1974 to regulate pension and welfare employee benefit plans that are established by private-sector employers, unions, or both, to provide benefits to their workers and dependents. An employee welfare benefit plan provides benefits—through insurance or otherwise—such as medical, surgical benefits, as well as benefits to cover accidents, disability, death, or unemployment. In 1996, HIPAA amended ERISA to require portability, nondiscrimination, and renewability of health benefits provided by group health plans and group health insurance issuers. Many, although not all, ERISA plans are covered under the proposed rule as health plans. We believe that the proposed rule does not conflict with ERISA. Further discussion of ERISA can be found in the preamble for this proposed rule.

E. Costs

Affected entities will be implementing the privacy proposed rules at the same time many of the administrative simplification standards are being implemented. As described in the overall impact analysis for the administrative simplification standards in the **Federal Register**, Vol. 63, No. 88, May 7, 1998, page 25344, the data handling changes occurring due to the other HIPAA standards will have both costs and benefits. To the extent the changes required for the privacy standards implementations can be made concurrently with the changes required for the other standards, costs for the combined implementation should be only marginally higher than for the administrative simplification standards alone. The extent of this additional cost is uncertain, in the same way that the costs associated with each of the individual administrative simplification standards was uncertain.

The costs associated with implementing the privacy standards will be directly related to the number of affected entities and the number of affected transactions in each entity.[17] We chose to use the SBA data in the RFA because we wanted our analysis to be as consistent to SBA definitions as possible to give the greatest accuracy for the RFA purposes. As described in the overall administrative simplification impact estimates (Tables 1 and 2, page 25344), about 20,000 health plans (excluding non-self administered employer plans)[18] and hundreds of thousands of providers face implementation costs. In the administrative simplification analysis, the costs of provider system upgrades were expected to be $3.6 billion over the period 1998–2002, and plan system cost upgrades were expected to be $2.2 billion. (In the aggregate, this $5.8 billion cost is expected to be more than completely offset by $7.3 billion in savings during the 5 year period analyzed).

The relationship between the HIPAA security and privacy standards is particularly relevant. On August 12, 1998, the Secretary published a proposed rule to implement the HIPAA standards on security and electronic standards. That rule specified the security requirements for covered entities that transmit and store information specified in Part C, Title XI of the Act. In general, that rule would establish the administrative and technical standards for protecting ''* * * any health information pertaining to an individual that is electronically maintained or transmitted.'' (63 FR 43243). The security rule is intended to spell out the system and administrative requirements that a covered entity must meet in order to assure itself and the Secretary that the protected health information is safe from destruction and tampering from people without authorization for its access.

By contrast, the privacy rule describes the policies and procedures that would govern the circumstances under which protected health information may be used and released with and without patient authorization and when a patient may have access to his or her protected medical information. This rule assumes that a covered entity will have in place the appropriate security apparatus to successfully carry out and enforce the provisions contained in the security rule.

Although the vast majority of health care entities are privately owned and operated, Federal, State, and local government providers are reflected in the total costs.[19] Federal, state, and locally funded hospitals represent approximately 26 percent of hospitals in the United States. This is a significant portion of hospitals, but represents a relatively small proportion of all

[17] We have used two different data sources for our estimates of the number of entities. In the regulatory impact analysis (RIA), we chose to use the same number of entities cited in the other Administrative Simplification rules. In the regulatory flexibility analysis (RFA), we used the most recent data available from the Small Business Administration (SBA).

We chose to use the Administrative Simplification estimates in the RIA because we wanted our analysis to be as consistent as possible with those regulations. We also believe that because the Administrative Simplification numbers are higher than those in the SBA data, it was the more conservative data source.

[18] We have not included the 3.9 million ''other'' employer health plans listed in HCFA's administrative simplification regulations because these plans that are administered by a third party. The proposed regulation will not regulate the employer-plans but will regulate the third party administrators of the plans. Because plan administrators have already been included in our analysis, these other employer-sponsored plans will not incur additional costs.

[19] These costs only represent those of public entities serving in the role of provider plan. The federal costs only reflect those incurred by a provider and plan offering Medicaid or Medicare, and hospitals run by the federal government including those run by the Veteran's Administration and the militry. Federal enforcement and other costs are not included. These estimates do not reflect any larger systems changes necessary to running federal programs. Likewise State costs are incorporated to the extent that States serve as providers or plans (including Medicaid).

provider entities. The number of government providers who are employed at locations other than government hospitals is significantly smaller (approximately 2 percent of all providers). Weighting the relative number of government hospital and non-hospital providers by the revenue these types of providers generate, we estimate that health care services provided directly by government entities represent 3.4 percent of total health care services. IHS and Tribal facilities costs are included in the total, since the adjustments made to the original private provider data to reflect federal providers included them. In drafting the proposed rule the Department consulted with States, representatives of the National Congress of American Indians, representatives of the National Indian Health Board, and a representative of the self-governance tribes. During the consultation we discussed issues regarding the application of Title II of HIPAA to the States and Tribes.

Estimating the costs associated with the privacy proposed rule involves, for each provision, consideration of both the degree to which covered entities must modify their records management systems and privacy policies under the proposed rule, and the extent to which there is a change in behavior of both patients and the covered entities as a result of the proposed rule. In the following sections we will examine these provisions as they would apply to the various covered entities as they undertake to comply with the proposed rule. The major costs that covered entities will incur are one time costs associated with implementation of the proposed rules, and ongoing costs that result from changes in behavior that both the covered entities and patients would make in response to the new proposed rules.

We have quantified the costs imposed by the proposed regulation to the extent that we had adequate data. In some areas, however, there was too little data to support quantitative estimates. As a result, the RIA does not include cost estimates for all of the requirements of the regulation. The areas for which explicit cost estimates have not be made are: The principle of minimum necessary disclosure; the requirement that entities monitor business partners with whom they share PHI; creation of de-identified information; internal complaint processes; sanctions; compliance and enforcement; the designation of a privacy official and creation of a privacy board; and additional requirements on research/optional disclosures that will be imposed by the regulation. The cost of some of these provisions may be significant, but it would be inaccurate to project costs for these requirements given the fact that several of these concepts are new to the industry.

The one time costs are primarily in the area of development and codification of procedures. Specific activities include: (1) Analysis of the significance of the federal regulations on covered entity operation; (2) development and documentation of policies and procedures (including new ones or modification of existing ones); (3) dissemination of such policies and procedures both inside and outside the organization; (4) changing existing records management systems or developing new systems; and (5) training personnel on the new policies and system changes.

Covered entities will also incur ongoing costs. These are likely to be the result of: (1) Increased numbers of patient requests for access and copying of their own records; (2) the need for covered entities to obtain patient authorization for uses of protected information that had not previously required an authorization; (3) increased patient interest in limiting payer and provider access to their records; (4) dissemination and implementation both internally and externally of changes in privacy policies, procedures, and system changes; and (5) training on the changes.

Compliance with the proposed rule will cost $3.8 billion over five years. These costs are in addition to the administrative simplification estimates. The cost of complying with the regulation represents 0.09 percent of projected national health expenditures the first year the regulation is enacted. The five year costs of the proposed regulation also represents 1.0 percent of the increase in health care costs experienced over the same five-year period.[20] Because of the uncertainty of the data currently available, the Department has made estimates on ''low'' and ''high'' range assumptions of the key variables. These estimates show a range of $1.8 to $6.3 billion over five years. It is important to note that these estimates do not include the areas for which we have made no cost estimates (discussed above).

Initial Costs

Privacy Policies and Procedures

With respect to the initial costs for covered entities, the expectation that most of the required HIPAA procedures will be implemented as a package suggests that additional costs for the privacy standards should be small. Since the requirements for developing formal processes and documentation of procedures mirror what will already have been required under the security regulations, the additional costs should be small. The expectation is that national and state associations will develop guidelines or general sets of processes and procedures and that these will generally be adopted by individual member entities. Relatively few providers or entities are expected to develop their own procedures independently or to modify significantly those developed by their associations. Our estimates are based on assumed costs for providers ranging from $300 to $3000, with the weighted average being about $375. The range correlates to the size and complexity of the provider, and is a reasonable estimate of the cost of coordinating the policies and procedures outlined in the proposed regulation. With fewer than 1 million provider entities, the aggregate cost would be on the order of $300 million.

For plans, our estimate assumes that the legal review and development of written policies will be more costly because of the scope of their operations. They are often dealing with a large number of different providers and may be dealing with requirements from multiple states. Again, we expect associations to do much of the basic legal analysis but plans are more likely to make individual adaptations. We believe this cost will range from $300 for smaller plans and $15,000 for the largest plans. Because there are very few large plans in relation to the number of small plans, the weighted average implementation costs will be about $3050.

The total cost of development of policies and procedures for providers and plans is estimated to be $395 million over five years.

System Compliance Costs

With respect to revisions to electronic data systems, the specific refinements needed to fulfill the privacy obligations ought to be closely tied to the refinements needed for security obligations. The overall administrative simplification system upgrades (procedures, systems, and training) of $5.8 billion would certainly be disproportionately associated with the security standard, relative to the other 11 elements. If in privacy it constitutes 15 percent, then the security standard would represent about $900 million system cost. If the marginal cost of the privacy elements is another 10 percent,

[20] Health Care Finance Administration, Office of the Actuary, 1997.

then the addition cost would be $90 million.

Ongoing Costs

The recurrent costs may be more closely related to total numbers of persons with claims than to the number of covered entities. The number of individuals served by an entity will vary greatly. The number of persons with claims will give a closer approximation of how many people entities will have to interact with for various provisions.

Notice of Privacy Practices

No State laws or professional associations currently require entities to provide patients ''notice'' of their privacy policies. Thus, we expect that all entities will incur costs developing and disseminating privacy policy notices. Each entity will have a notice cost associated with each person to whom they provide services. Data from the 1996 Medical Expenditure Panel Survey shows that there are approximately 200 million ambulatory care encounters per year, nearly 20 million persons with a hospital episode, 7 million with home-health episodes, and over 170 million with prescription drug use (350 million total). For the remaining four years of the five year period, we have estimated that, on average, a quarter of the remaining population will enter the system, and thus receive a notice. If we account for growth in the number of people who may enter the health care system over the five year period of our analysis, we estimate that approximately 543 million patients will be seen at least once by one or more types of providers.

The development cost for notices is estimated to cost $30 million over five years, though most of this is likely to occur the first year. The first year cost of providing notices to patients, customers and plan enrollees would be $106 million. The total five year cost of providing new and subsequent copies to all provider patients and customers would be approximately $209 million.

The notice obligations of insurers apply on initial enrollment, with updated notices at least every 3 years. However, given enrollment changes and the sophistication of automation, we believe many plans would find it cheaper and more efficient to provide annual notices.

The 1998 National Health Interview Survey (NHIS) from the Census Bureau shows about 174.1 million persons are covered by private health insurance, on an unduplicated basis. NHIS calculates that persons who are privately insured hold approximately 1.3 policies per person. Based on information provided by several plans, we believe most plans would provide an independent mailing the first year, but in subsequent years would provide notices as an inclusion in other mailings. The cost for this would be $0.75 over five years. If we account for these duplicate policies and assume that the cost of sending the notices to a policyholder is $0.75, the total cost to plans would be $231 million over five years. This includes both public and private plans.

We request comments regarding our cost estimates for development and distribution of notices.

The costs for more careful internal operation of covered entities to execute their formal privacy procedures are highly dependent on the extent to which current practice tracks the future procedures. Entities that already have strict data sharing and confidentiality procedures will incur minimal costs, since their activities need not change much. Entities that have not developed explicit health information privacy policies may be compelled to obtain patient authorization in situations where they did not previously. These changes will generate ongoing costs as well as initial costs. We solicit comment with respect to the way current costs differ from those projected by the requirements of the proposed privacy rule. An example of such an area is ''the minimum necessary disclosure principle''—because of differing current practices, we do not have data that reliably indicate how much this provision will cost.

Inspection and Copying

The Georgetown report on State privacy laws indicates that 33 states currently give patients some right to access medical information. The most common right of access granted by State law is the right to inspect personal information held by physicians and hospitals. In the process of developing estimates for the cost of providing access and copying, we assumed that most providers currently have procedures for allowing patients to inspect and copying their own record. Thus, we expect that the economic impact of requiring entities to allow individuals to access and copy their records should be relatively small. Copying costs, including labor, should be a fraction of a dollar per page. We expect the cost to be passed on to the consumer.

There are few studies that address the cost of providing medical records to patients. The most recent was a study in 1998 by the Tennessee Comtroller of the Treasury. It found an average cost of $9.96 per request, with an average of 31 pages per request. The total cost per page of providing copies was $0.32 per page. This study was performed on hospitals only. The cost per request may be lower for other types of providers, since those seeking hospital records are more likely to be sick and have more complicated records than those in a primary care or other type of office. An earlier report showed much higher costs than the Tennessee study. In 1992, Rose Dunn published a report based on her experience as a manager of medical records. She estimated a 10 page request would cost $5.32 in labor costs only, equaling labor cost per page of $0.53. However, this estimate appears to reflect costs before computerization. The expected time spent per search was 30.6 minutes; 85 percent of this time could be significantly reduced with computerization (this includes time taken for file retrieval, photocopying, and re-filing; file retrieval is the only time cost that would remain under computerization.) For subsequent estimates, we will use the Tennessee experience.

The proposed regulation states that entities may charge patients a reasonable fee to inspect and copy their health information. For this reason, we expect the cost of inspecting and copying an individual medical record to be passed on to consumers who request the service. Nonetheless, it is important to provide an estimate of the potential costs associated with inspection and copying. We assume that 1.5 percent of patients will request access to inspect and copy their medical record, and that the cost of accessing and copying a record is approximately $10 (as cited in the Tennessee study). The cost of inspection and copying is $81 million a year, or $405 million over five years. This cost is likely to be borne entirely by the consumer.

Amendment and Correction

We have assumed that many providers make provisions to help patients expedite amendment and correction of their medical record where appropriate. However, as with inspection and copying, the right to request amendment and correction of an individual's medical record is not guaranteed by all States. Based on these assumptions and our cost analysis, we conclude that the principal economic effect of the proposed rule would be to expand the right to request amendment and correction to plans and providers that are not covered by state laws or codes of conduct. In addition, we expect that the proposed rule may draw additional attention to the issue of record inaccuracies and stimulate